

云计算时代企业信息安全攻略必读！
信息安全
保卫战
企业信息安全建设
策略与实践
雷万云 等著
基于云计算理念，本书提出一个组织的整体安全框架，从组织的战略、业务出发，结合安全标准和业界最佳实践，形成系统的信息安全建设方法路径。
帮助组织定位安全现状，了解安全需求，实施安全建设，以打赢信息安全保卫战。

清华大学出版社

信息安全保卫战

——企业信息安全建设策略与实践

雷万云　等著

清华大学出版社
北　京

内 容 简 介

本书定位于一个组织信息安全建设理论、技术、策略方法以及实践案例的介绍和论述，描述当今信息化社会环境下，如何打赢信息安全保卫战。全书分为 11 章，首先综述了信息化社会的信息安全威胁，说明打赢信息安全保卫战的重要意义。其次论述了信息安全发展历程和信息安全标准以及云计算安全发展状况。再次，提出了企业信息安全框架的概念和内容，最后给出了一个组织信息安全框架建设的策略与方法以及实践案例，帮助读者形成信息安全建设的思路和系统的方法路径以及最佳实践。

本书面向组织的管理者、CIO 和从事信息化、信息安全建设的 IT 人；其次是咨询公司的业务和 IT 咨询人员以及企业信息安全项目实施人员。对于大专院校的师生们进一步系统地认识企业信息安全建设、形成科学系统的信息安全建设思路是一个绝好的参考书。

图书在版编目（CIP）数据

信息安全保卫战：企业信息安全建设策略与实践 / 雷万云等编著. —北京：清华大学出版社，2013.1

ISBN 978-7-302-30915-4

Ⅰ. ①信…　Ⅱ. ①雷…　Ⅲ. ①企业管理–信息系统–安全管理　Ⅳ. ①F270.7

中国版本图书馆 CIP 数据核字（2012）第 286764 号

责任编辑： 夏兆彦
封面设计： 柳晓春
责任校对： 徐俊伟
责任印制：

出版发行： 清华大学出版社
　网　　址：http://www.tup.com.cn, http://www.wqbook.com
　地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
　社 总 机：010-62770175　　邮　　购：010-62786544
　投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
　质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 刷 者：
装 订 者：
经　　销： 全国新华书店
开　　本： 190mm×260mm　　**印　张：** 17　　**字　数：** 372 千字
版　　次： 2013 年 1 月第 1 版　　**印　次：** 2013 年 1 月第 1 次印刷
印　　数：
定　　价： 　　元

产品编号：046188-01

前　言

社会信息化，已成不可阻挡的历史潮流，成为大趋势，引发可怕的信息安全威胁。可以看到，随着新一代信息技术的飞速发展和应用，给我们带来好处的同时，也相应地给我们带了前所未有的信息安全威胁。信息安全逐渐告别传统的病毒感染、网站被黑及资源滥用等时代，迈进了一个复杂多元、综合交互的新时期。如何在有效利用信息技术的同时，积极应对和及时识别和规避这些风险，形成新的信息安全建设策略与实践，打好信息安全保卫战，是我们大家必须面对的主题，也是本书讨论和论述的话题。

《信息安全保卫战》是笔者有关企业信息化建设系列丛书之一，她的出版和近年来笔者在清华大学出版社出版的《云计算——企业信息化建设策略与实践》、《云计算——技术、平台及应用案例》以及《信息化与信息管理实践之道》构成一个完整的企业信息化建设四部曲。第一本云计算是云计算的普及图书，全面系统地论述了云计算的概念、技术以及市场发展状况，并在此基础上进一步阐述基于云计算的企业信息化建设策略与实践。第二本云计算是在第一本基础上深入阐述云计算的概念、技术和架构以及国内外的应用案例。第三本是有关企业信息化与信息管理的实战图书，从信息化规划、管控、标准和项目实施等层面论述企业信息化建设的策略、方法与实践。第四本也就是本书是对信息安全这一主题的全面深入论述。

本书基于云计算理念，提出一个组织的整体安全概念，从组织的战略、业务出发，结合安全标准和业界最佳实践，形成系统的方法路径，帮助组织定位安全现状，了解安全需求，实施安全建设，以打赢我们的信息安全保卫战。目前业界已有众多的信息安全书籍，但大都是针对某一系统的信息安全具体的技术探讨。本书旨在对一个组织信息安全建设提供一个集成的、标准的信息安全框架，为组织信息安全平台的建设、设计、实施提供指导。全书为 11 章，其主要内容如下。

第 1 章首先从全球一体化、信息技术的发展利用等方面综述了信息化社会的信息安全威胁，并进一步阐述了企业信息化的发展应用对企业信息安全带来的威胁。第 2 章通过企业合规经营风险分析引入企业风险与信息安全的关系，说明信息安全是确保企业合规经营的基本保障。第 3 章在分析企业信息安全现状的基础上进一步论述了企业信息安全建设的目的意义，说明打赢信息安全保卫战的重要性。

第 4 章介绍了信息安全发展历程和国内外信息安全标准。第 5 章在分析云计算安全问题基础上进一步提出了云计算安全框架，并论述了云计算安全标准的发展情况，最后进一步综述了国内外先进的云计算安全提供商的云计算安全解决方案。

第 6 章引入企业信息安全框架概念，并全面、完整地阐述了企业信息安全框架的定义、内容以及建设意义。第 7、8、9 章分别对信息安全框架的三个组成部分：信息安全管理、运维和技术体系深入介绍和描述。

第 10 章从一个组织的战略出发来全面考虑组织的信息安全的规划、管理、技术、运维等完整的信息安全框架设计与实施的策略与方法并进行了系统论述，给出一个信息安全框架建设的方法和路径，第 11 章并给出了相应的实践案例。

本书定位于一个组织（包括政府、区域和城市、企业等）信息安全建设理论、技术、策略方法以及实践案例介绍和论述，从系统工程层面来论述，体现企业信息安全建设的方法论。

本书主要面向企业的 CEO 和企业管理人员，企业的 CIO 和从事信息化、信息安全建设的 IT 人；其次是咨询公司的业务和 IT 咨询人员以及企业信息安全项目实施人员；当然对于政府的管理人员来讲，是一个很好的信息安全知识水平和工作思路的提升学习的最佳参考书；对于大专院校的师生们进一步系统地认识企业信息安全建设、企业 IT 的实际情况，企业和社会信息安全建设思路是一个绝好的参考书；最后，对于从事企业信息安全的服务提供商也是一个很好的值得借鉴的参考书，因为只有深刻了解企业的需求、信息安全建设的系统思维，才能实施好企业信息安全项目。

本书由雷万云博士主持编写，华为技术公司、启明星辰信息安全公司和深信服科技公司相关专家参加了编写。他们分别是：华为企业网安全首席技术官何利文，IEEE 高级会员，全国青联 IT 联谊会常务理事，英国谢菲尔德大学博士，曾任英国电信首席安全研究员；华为数据中心安全高级营销顾问时成阁；华为企业网安全高级营销顾问黄菲一。启明星辰信息安全高级咨询顾问刘德文和张艳博士。深信服科技市场技术总监殷浩先生。雷万云博士撰写了大纲和各章节的主要内容要点，对全书各章节内容进行了优化、统稿和对全部内容进行了审阅，并撰写了前言。其中第 1 章、第 3 章和第 4 章由雷万云博士撰写；第 2 章由雷万云博士、王静撰写；第 5 章由雷万云博士、何利文、黄菲一撰写；第 6 章由雷万云博士、刘德文、张艳博士撰写；第 7 章由刘德文、雷万云博士、张艳撰写；第 8 章由何利文、时成阁、刘德文、雷万云博士撰写；第 9 章由何利文、时成阁、雷万云博士、殷浩撰写；第 10 章由雷万云博士、刘德文、张艳编写，第 11 章由雷万云博士、刘德文、张艳、殷浩编写。李懿凌和韩金利画了书中的大部分示图。

由于作者水平有限，书中难免有疏漏和不当之处，敬请读者批评指正。有什么建议和意见可以在我的新浪博客：http://blog.sina.com.cn/alexalei 留言互动或写信到我的邮箱：leiwy@sinopharm.com。

最后，谨向帮助、支持和鼓励我完成本书的我的家人、同事、领导、朋友、合作伙伴以及清华出版社的领导、编辑表示真挚的感谢！

雷万云 博士

2012 年国庆假期于北京

目 录

第1章 信息化社会的信息安全威胁

信息化社会的发展带来了前所未有的信息安全威胁，信息安全战的硝烟弥漫着整个地球，企业的信息安全保卫战号角已经吹响。本章分四节论述了信息化社会的信息安全威胁。首先从社会信息化的趋势和新 IT 技术应用带来的新风险给我们说明信息化是世界发展的大趋势，并给我们带来了严重的信息安全威胁；其次论述了信息化与全球一体化发展的交融、互动趋势以及信息安全威胁；接着论述了信息化也是企业发展与竞争的必然趋势，因而使得企业信息安全无法回避；最后从五个层次总结、描述了信息化社会给我们带来的信息安全威胁状况。

1.1 信息化是世界发展的大趋势

纵观社会生产方式经历的三次变革，从农业时代、工业时代到现在的信息时代。在信息时代，主要是多元的协同化生产方式，通过信息化使分散与集中实现协同发展。随着全球经济一体化的步伐加快，代表着信息时代已悄然而至，云计算是工业化后最重要的一次变革，信息化是世界发展的大趋势。然而，在我们享受着信息化带来好处的同时，也感觉到信息安全的威胁。

1.1.1 社会信息化的趋势

社会信息化，已成不可阻挡的历史潮流，成为大趋势，引发可怕的信息安全威胁。信息化是充分利用信息技术，开发利用信息资源，促进信息交流和知识共享，提高经济增长质量，推动经济社会发展转型的历史进程。20 世纪 90 年代以来，信息技术不断创新，信息产业持续发展，信息网络广泛普及，信息化成为全球经济社会发展的显著特征，并逐步向一场全方位的社会变革演进。进入 21 世纪，计算机与互联网的迅猛发展给人们的生活方式、商业贸易的交易方式以及政府的运作方式、军队的作战方式等都带来了革命性的变化，加快了国家现代化和社会文明的发展。广泛应用、高度渗透的信息技术正孕育着新的重大突破。信息资源日益成为重要生产要素、无形资产和社会财富，信息网络

更加普及并日趋融合。信息化与经济全球化相互交织，推动着全球产业分工深化和经济结构调整，重塑着全球经济竞争格局。互联网加剧了各种思想文化的相互激荡，成为信息传播和知识扩散的新载体。电子政务在提高行政效率、改善政府效能、扩大民主参与等方面的作用日益显著。信息化使现代战争形态发生重大变化，是世界新军事变革的核心内容。然而，信息技术在为人们提供便捷、高效服务的同时，也对依赖其运行的国家、企业关键信息系统和基础信息网络设施带来了巨大的风险。由于信息技术本身的特殊性，特别是信息和网络无国界的特点，信息安全问题已成为信息社会发展的一大挑战。传统的信息安全已被彻底改写，信息安全不仅是一个技术问题，而且是一个管理与控制问题，它涉及到国家安全、社会公共安全、企业经营安全以及公民个人安全的方方面面，是一个事关国家根本利益的战略问题。

信息安全的重要性与日俱增，成为各国面临的共同挑战。全球数字鸿沟呈现扩大趋势，发展失衡现象日趋严重。发达国家信息化发展目标更加清晰，正在出现向信息社会转型的趋向；越来越多的发展中国家主动迎接信息化发展带来的新机遇，力争跟上时代潮流。全球信息化正在引发当今世界的深刻变革，重塑世界政治、经济、社会、文化和军事发展的新格局。持续、稳健、深入地推动信息安全建设，已经成为世界各国的共同选择。

1.1.2 新 IT 技术应用带来新风险

从信息技术的长期演进趋势来看，中国目前仍然处于蓬勃发展的阶段，下一代互联网、无线宽带技术、传感网、新型显示和云计算技术等信息技术和应用表现出新的发展趋势和动向，通过与当前经济和社会发展的各项工作相结合，将进一步提升社会生产效率，提升传统产业发展的竞争力，产生一批新兴产业，促进社会生产和生活方式等方方面面的变革，为经济结构调整起到重要作用，并将成为今后一个阶段经济结构调整的重要方向。

然而，在互联网为我们带来了更平、更小、更智慧的地球，使我们的联系和信息传递更加紧密，互联互通程度更高的同时，也给我们带来前所未有的信息安全威胁。这是由于新的技术带来了数十亿计的移动设备、实时的信息交流以及更加紧密、更加多样化的协作方式，这些新技术的大规模应用一方面提供了智慧的能力，另一方面也带来了新的风险。

云计算作为下一代信息技术的主要代表，是通过 10 年互联网技术和应用演进而产生的，这一大规模的计算能力通常是由分布式的大规模集群和服务器虚拟化软件搭建而成的。云计算为用户提供了一个颠覆性的服务交付模式，是全球经济一体化的解决方案。云计算提供了无限的规模和差异化的服务，简化了服务的交付。特别是在智慧城市、物联网这样的大背景下，许多组织、企业希望也需要通过云计算培养快速创新和应变能力，引领企业的转型升级，以便可以在当今高度竞争的环境中快速地作出应对，同时还通过云计算降低企业运营

成本。此外，云计算还提供了一个可伸缩的环境，以便轻松有效地满足客户的需要。

在云计算带来创新能力、创造众多市场机会的同时，信息专家们还没有忘记提醒用户“云计算有风险、入云需谨慎”。研究机构 Gartner 曾发布了一份名为《云计算安全风险评估》的报告。报告中指出，云计算需要进行安全风险评估的领域包括数据完整性、数据恢复及隐私等。此外，还需对电子检索、可监管性及审计问题进行法律方面的评价。报告同时列出了云计算技术面临的七大风险，包括特权用户的接入、可审查性、数据位置、数据隔离、数据恢复、调查支持、长期生存性。

在云计算面前，信息安全产业似乎正陷入一个矛盾的境地：一方面，企业因为安全问题而对云计算应用敬而远之；另一方面，由于缺少用户，云安全产业暂时无法迎来行业契机。特别是在关键数据和隐私方面，希望实现“云”可管可控，“如果安全问题没有解决，那么‘云’将无法在现实中落地。”

可以看到，随着新一代信息技术的飞速发展和应用，给我们带来好处的同时，也相应地给我们带了前所未有的信息安全威胁。信息安全逐渐告别传统的病毒感染、网站被黑及资源滥用等时代，迈进了一个复杂多元、综合交互的新时期。如何在有效利用信息技术的同时，积极应对、及时识别和规避这些风险，形成新的信息安全建设策略与实践，打好信息安全保卫战，是我们大家必须面对的主题，也是本书讨论和论述的话题。

1.2　全球一体化的趋势

社会信息化大大缩小了世界的时间和空间范围，使地球世界变成了“地球村”，为经济全球化提供了有效的经济信息平台和经济活动空间。社会信息化、交通现代化、人员知识化、生产自动化、产品标准化、工作程序化、地域一体化、生活服务化，造就了经济全球化的良好环境，大民生、大需求、大贸易、大智慧、大服务、高技术、大合作、大发展，成为经济全球化发展的最大推动力！

经济全球化趋势，日益明显、势不可挡。经济全球化形成和促进了汹涌澎湃的商品流、资金流、资源流、技术流、信息流、人流、物流的全球流量；经济是基础，全球经济信息流量，对世界各国形成巨大的冲击力，不断冲击各国社会政治、文化、科技、军事、工业、农业、旅游业、服务业的发展，使世界各行业在发展中融合，在融合中，超越国界，弱化国界，模糊国界，特别是以人为本的“民生经济”受各国青睐，人们期盼的是民生、和谐、幸福！

面对经济全球化、社会信息化的趋势，我国信息化发展的对策是：贯彻落实科学发展观，坚持以信息化带动工业化、以工业化促进信息化，坚持以改革开放和科技创新为动力，大力推进信息化，充分发挥信息化在促进经济、政治、

文化、社会和军事等领域发展的重要作用，不断提高国家信息化水平，走中国特色的信息化道路，促进我国经济社会又快又好地发展。

面对汹涌袭来的信息安全威胁，国家也提出了全面加强国家信息安全保障体系建设的举措。坚持积极防御、综合防范，探索和把握信息化与信息安全的内在规律，主动应对信息安全挑战，实现信息化与信息安全协调发展。坚持立足国情，综合平衡安全成本和风险，确保重点，优化信息安全资源配置。建立和完善信息安全等级保护制度，重点保护基础信息网络和关系国家安全、经济命脉、社会稳定的重要信息系统。加强密码技术的开发利用，建设网络信任体系。加强信息安全风险评估工作，建设和完善信息安全监控体系，提高对网络安全事件应对和防范能力，防止有害信息传播。高度重视信息安全应急处置工作，健全完善信息安全应急指挥和安全通报制度，不断完善信息安全应急处置预案。从实际出发，促进资源共享，重视灾难备份建设，增强信息基础设施和重要信息系统的抗毁能力和灾难恢复能力。

大力增强国家信息安全保障能力。积极跟踪、研究和掌握国际信息安全领域的先进理论、前沿技术和发展动态，抓紧开展对信息技术产品漏洞、后门的发现研究，掌握核心安全技术，提高关键设备装备能力，促进我国信息安全技术和产业的自主发展。加快信息安全人才培养，增强国民信息安全意识。不断提高信息安全的法律保障能力、基础支撑能力、网络舆论宣传的驾驭能力和我国在国际信息安全领域的影响力，建立和完善维护国家信息安全的长效机制。

1.3 企业发展与竞争的趋势

面对这个精彩世界，全球经济一体化进程浪潮以及互联网技术的成熟和迅猛发展，使企业所处的竞争环境和发展空间发生了许多变化。根据 2011 年 Gartner 公司的分析报告显示，企业在新环境下，最关注的业务问题包括加快企业增长、降低成本、优化业务流程、升级业务应用、改善技术架构、提高企业效率等；最关注的技术问题包括云计算、移动技术、商务智能、协同等；而对企业架构影响最大的则是虚拟化。快速发展与新技术使用的情况说明，企业为适应快速变化的环境，需要利用 IT 改变过去传统的很多看法，需要利用最新的技术（如虚拟化等技术趋势），向构建一个可以不断更新的战略规划方向和企业构架努力。

从企业角度来看，由于在新的经济环境下企业需要在战略与发展方面参与全球化和国内跨区域的各种竞争，促使企业在管理与运作方面不断推出和适应新的模式和理念：企业从“做大做强”转向“做强做优”。企业的眼界与实践也快速向全球化、精益化、协同化、服务化和智能化五大发展趋势顺应发展，集团企业的管控工作也逐步从财务管控转向精细化的运营管控和全球化的战略管控发展，总部职能更加强调向协同、共享、服务等转变。面对复杂多变的内外

部环境带来的挑战，企业必须具备快速决策、协同运营、控制风险及高效发展的能力，需要企业对信息化建设工作的方向和目标不断提出新的全方位的要求，才能推动更深入的应用。因此，强调信息化与新的商业运作模式融合，迅速顺应信息技术发展，通过以网络服务及流程管理技术在企业的应用为先导，推动企业的管理变革和信息化建设工作，是新环境下企业面对内外部变化而必须采用的对策。互联化、物联化、虚拟化、智能化已经成为企业必须跟进的新一代信息技术创新应用趋势。

面对经济全球一体化和激烈的市场竞争环境，企业信息化发展也趋于信息一体化、网络化、互联化以及向云演进的趋势，同时也面临着更加恶劣的信息安全威胁和风险。因此，打好企业信息安全保卫战，做好企业信息安全建设是企业运作发展的基本保障。

1.4　信息安全威胁综述

作为 20 世纪最伟大的科学技术创造之一，互联网已经成为世界各国人民沟通的重要工具。进入 21 世纪，以互联网为代表的信息化浪潮席卷世界每个角落，渗透到经济、政治、文化和国防等各个领域，对人们的生产、工作、学习、生活等产生了全面而深刻的影响，也使世界经济和人类文明跨入了新的历史阶段。然而，伴随着互联网的飞速发展，网络信息安全问题日益突出，越来越受到社会各界的高度关注。如何在推动社会信息化进程中加强网络与信息安全管理，维护互联网各方的根本利益和社会和谐稳定，促进经济社会的持续健康发展，成为我们在信息化时代必须认真解决的一个重大问题。

1.4.1　信息安全面临的主要威胁

飞速发展的互联网业在给社会和公众创造效益、带来方便的同时，其系统的漏洞和网络的开放性也给国家的经济建设和企业发展以及人们的社会生活带来了负面影响，病毒侵袭、网络欺诈、信息污染、黑客攻击等问题更是给我们带来困扰和危害。

计算机网络所面临的威胁主要有对网络中信息的威胁和对网络中设备的威胁两种。影响计算机网络的因素有很多，其所面临的威胁也就来自多个方面，主要威胁如图 1-1 所示。

（1）人为的失误：如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享都会对网络安全带来威胁。

（2）信息截取：通过信道进行信息的截取，获取机密信息，或通过信息的流量分析，通信频度、长度分析，推出有用信息，这种方式不破坏信息的内容，不易被发现。这种方式是在过去军事对抗、政治对抗和当今经济对抗中最常用

的，也是最有效的方式。

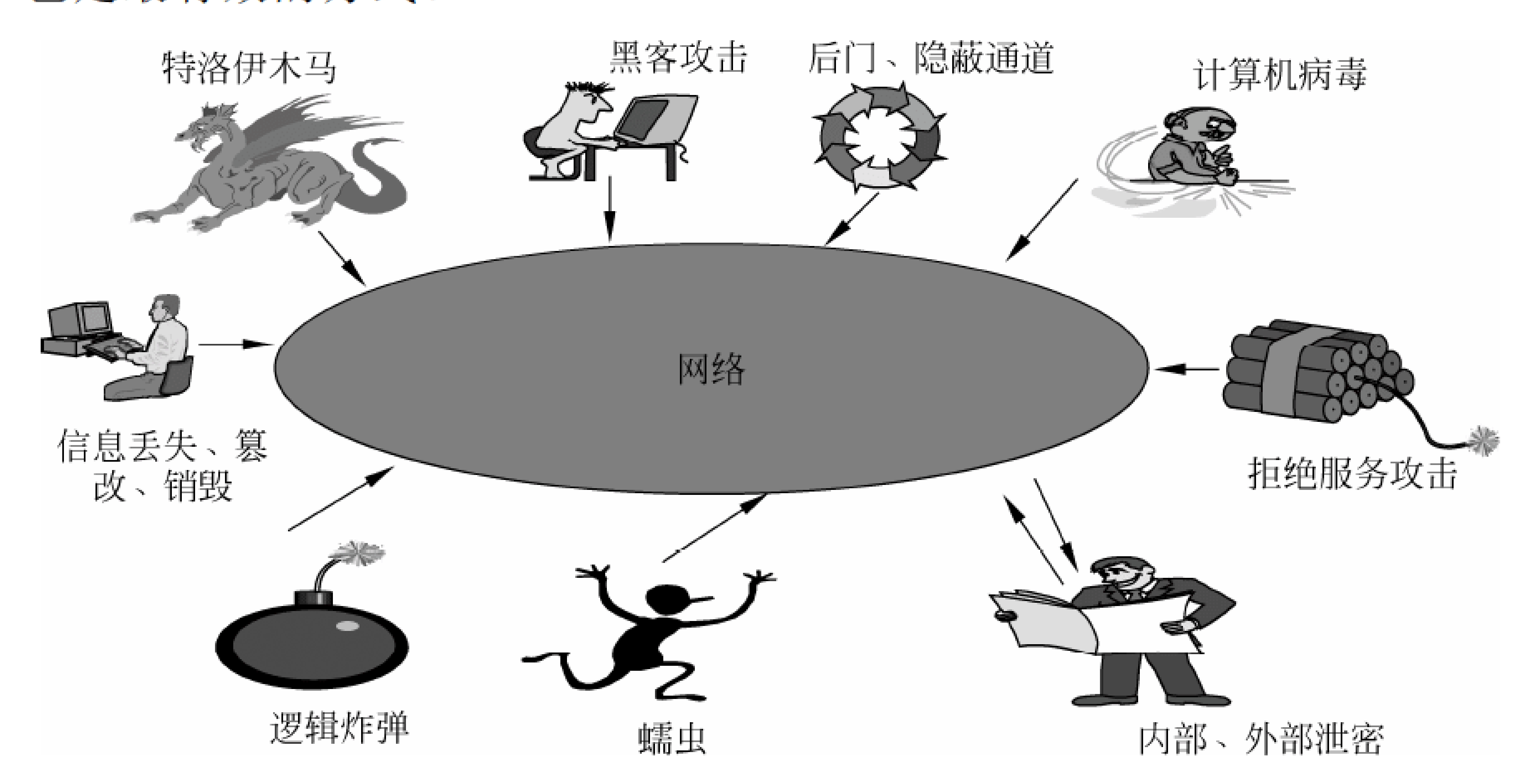


图 1-1 信息安全面临的威胁类型

（3）内部窃密和破坏：内部或本系统的人员通过网络窃取机密、泄露或更改信息以及破坏信息系统。据美国联邦调查局的一项调查显示，70%的攻击是从内部发动的，只有 30%是从外部攻进来的。

（4）黑客攻击：黑客已经成为网络安全的最大隐患。近年来，特别是 2000 年 2 月 7～9 日，美国著名的雅虎、亚马逊等八大顶级网站接连遭受来历不明的电子攻击，导致服务系统中断，这次攻击给这些网站造成的直接损失达 12 亿美元，间接经济损失高达 10 亿美元。

（5）技术缺陷：由于认识能力和技术发展的局限性，在硬件和软件设计过程中，难免留下技术缺陷，由此可造成网络的安全隐患。其次，网络硬件、软件产品多数依靠进口，如全球 90%的微机都装微软的 Windows 操作系统，许多网络黑客就是通过微软操作系统的漏洞和后门而进入网络的，这方面的报道经常见诸于报端。

（6）病毒：从 1988 年报道的第一例病毒（蠕虫病毒）侵入美国军方互联网，导致 8500 台计算机染毒和 6500 台停机，造成直接经济损失近 1 亿美元，此后这类事情此起彼伏，从 2001 年红色代码到 2012 年的冲击波和震荡波等病毒发作的情况看，计算机病毒感染方式已从单机的被动传播变成了利用网络的主动传播，不仅带来网络的破坏，而且造成网上信息的泄露，特别是在专用网络上，病毒感染已成为网络安全的严重威胁。另外，对网络安全的威胁还包括自然灾害等不可抗力因素。

对以上计算机网络的安全威胁归纳起来常表现为以下特征：

（1）窃听：攻击者通过监视网络数据获得敏感信息；

（2）重传：攻击者先获得部分或全部信息，而以后将此信息发送给接受者；

（3）伪造：攻击者将伪造的信息发送给接受者；

（4）篡改：攻击者对合法用户之间的通信信息进行修改、删除、插入，再

发送给接受者；

（5）拒绝服务攻击：供给者通过某种方法使系统响应减慢甚至瘫痪，阻碍合法用户获得服务；

（6）行为否认：通信实体否认已经发生的行为；

（7）非授权访问：没有预先经过同意，就使用网络或计算机资源；

（8）传播病毒：通过网络传播计算机病毒，其破坏性非常高，而且用户很难防范。

1.4.2　信息安全问题分析

目前政府部门、金融部门、企业单位的业务依赖于信息系统安全运行，信息安全重要性日益凸显。企业信息资源已经成为企业的重要财富和资源，企业如何保护信息安全和网络安全，最大限度地减少或避免因信息泄密、破坏等安全问题所造成的经济损失及对企业形象的影响，是摆在我们面前亟需妥善解决的一项具有重大战略意义的课题。目前有 15 个典型的信息安全问题急需解决。

1．网络共享与恶意代码防控

网络共享方便了不同用户、不同部门、不同单位等之间的信息交换，但是，恶意代码利用信息共享、网络环境扩散等漏洞，影响越来越大。如果对恶意信息交换不加限制，将导致网络的服务质量（QoS）下降，甚至系统瘫痪不可用。

2．信息化建设超速与安全规范不协调

网络安全建设缺乏规范操作，常常采取“亡羊补牢”之策，导致信息安全共享难度递增，也留下安全隐患。

3．信息产品国外引进与安全自主控制

国内信息化技术严重依赖国外，从硬件到软件都不同程度地受制于人。目前，国外厂商的操作系统、数据库、中间件、办公文字处理软件、浏览器等基础性软件都大量地部署在国内的关键信息系统中，但是这些软件或多或少存在一些安全漏洞，使得恶意攻击者有机可乘。目前，我们国家的大型网络信息系统许多关键信息产品长期依赖于国外，一旦出现特殊情况，后果就不堪设想了。

4．IT 产品单一性和大规模攻击问题

信息系统中软硬件产品单一性，如同一版本的操作系统、同一版本的数据库软件等，这样一来攻击者可以通过软件编程，实现攻击过程的自动化，从而常导致大规模网络安全事件的发生，如网络蠕虫、计算机病毒、“零日”攻击等安全事件。

5. IT 产品类型繁多和安全管理滞后矛盾

目前，信息系统部署了众多的 IT 产品，包括操作系统、数据库平台、应用系统。但是不同类型的信息产品之间缺乏协同，特别是不同厂商的产品，不仅产品之间安全管理数据缺乏共享，而且各种安全机制缺乏协同，各产品缺乏统一的服务接口，从而造成信息安全工程建设困难，系统中安全功能重复开发，安全产品难以管理，也给信息系统管理留下安全隐患。

6. IT 系统复杂性和漏洞管理

多协议、多系统、多应用、多用户组成的网络环境复杂性高，存在难以避免的安全漏洞。据 Security Focus 公司的漏洞统计数据表明，绝大部分操作系统存在安全漏洞。由于管理、软件工程难度等问题，新的漏洞不断地引入到网络环境中，所有这些漏洞都将可能成为攻击切入点，攻击者可以利用这些漏洞入侵系统，窃取信息。1998 年 2 月，黑客利用 Solar Sunrise 漏洞入侵美国国防部网络，受害的计算机数超过 500 台，而攻击者只是采用了中等复杂工具。当前安全漏洞时刻威胁着网络信息系统的安全。

为了解决来自漏洞的攻击，一般通过打补丁的方式来增强系统安全。但是，由于系统运行不可间断性及漏洞修补风险不可确定性，即使发现网络系统存在安全漏洞，系统管理员也不敢轻易地安装补丁。特别是，大型的信息系统，漏洞修补是一件极为困难的事。因为漏洞既要做到修补，又要能够保证在线系统正常运行。

7. 网络攻击突发性和防范响应滞后

网络攻击者常常掌握主动权，而防守者则被动应付。攻击者处于暗处，而攻击目标则处于明处。以漏洞的传播及利用为例，攻击者往往先发现系统中存在的漏洞，然后开发出漏洞攻击工具，最后才是防守者提出漏洞安全对策。

8. 口令安全设置和口令易记性难题

在一个网络系统中，每个网络服务或系统都要求不同的认证方式，用户需要记忆多个口令，据估算，用户平均至少需要 4 个口令，特别是系统管理员，需要记住的口令就更多了，如开机口令、系统进入口令、数据库口令、邮件口令、Telnet 口令、FTP 口令、路由器口令、交换机口令等。按照安全原则，口令设置既要求复杂，而且口令长度要足够长，但是口令复杂则记不住，因此，用户选择口令只好用简单的、重复使用的口令，以便于保管，这样一来攻击者只要猜测到某个用户的口令，就极有可能引发系列口令泄露事件。

9. 远程移动办公和内网安全

随着网络普及，移动办公人员在大量时间内需要从互联网上远程访问内部

网络。由于互联网是公共网络，安全程度难以得到保证，如果内部网络直接允许远程访问，则必然带来许多安全问题，而且移动办公人员计算机又存在失窃或被非法使用的可能性。“既要使工作人员能方便地远程访问内部网，又要保证内部网络的安全。”就成了一个许多单位都面临的问题。

10．内外网络隔离安全和数据交换方便性

由于网络攻击技术不断增强，恶意入侵内部网络的风险性也相应急剧提高。网络入侵者可以渗透到内部网络系统，窃取数据或恶意破坏数据。同时，内部网的用户因为安全意识薄弱，可能有意或无意地将敏感数据泄露出去。为了实现更高级别的网络安全，有的安全专家建议，“内外网及上网计算机实现物理隔离，以求减少来自外网的威胁。”但是，从目前网络应用来说，许多企业或机构都需要从外网采集数据，同时内网的数据也需要发布到外网上。因此，要想完全隔离开内外网并不太现实，网络安全必须既要解决内外网数据交换需求，又要能防止安全事件出现。

11．业务快速发展与安全建设滞后

在信息化建设过程中，由于业务急需要开通，做法常常是“业务优先，安全靠边”，使得安全建设缺乏规划和整体设计，留下安全隐患。安全建设只能是“亡羊补牢”，出了安全事件后才去做。这种情况，在企业中表现得更为突出，市场环境的动态变化，使得业务需要不断地更新，业务变化超过了现有安全保障能力。

12．网络资源健康应用与管理手段提升

复杂的网络世界，充斥着各种不良信息内容，常见的就是垃圾邮件。在一些企业单位中，网络的带宽资源被员工用来在线聊天，浏览新闻娱乐、股票行情、色情网站，这些网络活动严重消耗了带宽资源，导致正常业务得不到应有的资源保障。但是，传统管理手段难以适应虚拟世界，网络资源管理手段必须改进，要求能做到“可信、可靠、可视、可控”。

13．信息系统用户安全意识差和安全整体提高困难

目前，普遍存在“重产品、轻服务，重技术、轻管理，重业务、轻安全”的思想，“安全就是安装防火墙，安全就是安装杀毒软件”，人员整体信息安全意识不平衡，导致一些安全制度或安全流程流于形式。典型的事例如下：

用户选取弱口令，使得攻击者可以从远程直接控制主机；

用户开放过多网络服务，例如，网络边界没有过滤掉恶意数据包或切断网络连接，允许外部网络的主机直接“ping”内部网主机，允许建立空连接；

用户随意安装有漏洞的软件包；

用户直接利用厂家默认配置；

用户泄露网络安全敏感信息，如 DNS 服务配置信息。

14．安全岗位设置和安全管理策略实施难题

根据安全原则，一个系统应该设置多个人员来共同负责管理，但是受成本、技术等限制，一个管理员既要负责系统的配置，又要负责安全管理，安全设置和安全审计都是“一肩挑”。这种情况使得安全权限过于集中，一旦管理员的权限被人控制，极易导致安全失控。

15．信息安全成本投入和经济效益回报可见性

由于网络攻击手段不断变化，原有的防范机制需要随着网络系统环境和攻击适时而变，因而需要不断地进行信息安全建设资金投入。但是，一些信息安全事件又不同于物理安全事件，信息安全事件所产生的经济效益往往是间接的，不容易让人清楚明白，从而造成企业领导人的误判，进而造成信息安全建设资金投入困难。这样一来，信息安全建设投入往往是“事后”进行，即当安全事件产生影响后，企业领导人才会意识到安全的重要性。这种做法造成信息安全建设缺乏总体规划，基本上是“头痛医头，脚痛医脚”，信息网络工作人员整天疲于奔命工作，成了“救火队员”。

信息安全问题再次被整个行业提到了前所未有的高度，安全问题是整个信息技术行业的重中之重。

1.4.3 信息安全管理现状分析

（1）目前我国信息安全管理现状仍还比较混乱，对于国家、行业和企业都普遍缺乏一个战略层面的体系。实际管理力度不够，政策的执行和监督力度不够。部分规定过分强调部门的自身特点，而忽略了在国际政治经济的大环境下体现中国的特色。部分规定没有准确地区分技术、管理和法制之间的关系，以管代法，用行政管技术的做法仍较普遍，造成制度的可操作性较差。

（2）具有我国特点的、动态的和涵盖组织机构、文件、控制措施、操作过程、程序以及相关资源等要素的信息安全管理体系还未建立起来。

（3）具有我国特点的信息安全风险评估标准体系还有待完善，信息安全的需求难以确定，要保护的对象和边界难以确定，缺乏系统、全面的信息安全风险评估和评价体系以及全面、完善的信息安全保障体系。

（4）信息安全意识缺乏，普遍存在重产品、轻服务，重技术、轻管理的思想。

（5）专项经费投入不足，管理人才极度缺乏，基础理论研究和关键技术薄弱，严重依赖国外，对引进的信息技术和设备缺乏保护信息安全所必不可少的有效管理和技术改造。

（6）技术创新不够，信息安全管理产品水平和质量不高，尤其是以集中配置、集中管理、状态报告和策略互动为主要任务的安全管理平台产品的研究与

开发还很落后。

（7）缺乏权威、统一、专门的组织、规划、管理和实施协调的立法管理机构，致使我国现有的一些信息安全管理方面的法律法规层次不高，真正的法律少，行政规章多，结构不合理，不成体系；执法主体不明确，多头管理，政出多门、各行其是，规则冲突，缺乏可操作性，执行难度较大，有法难依；数量上不够，内容上不完善，制定周期太长，时间上滞后，往往无法可依；监督力度不够，有法不依、执法不严；缺乏专门的信息安全基本大法，如信息安全法和电子商务法等；缺乏民事法方面的立法，如互联网隐私法、互联网名誉权、网络版权保护法等；公民的法律意识较差，执法队伍薄弱，人才匮乏。

（8）我国自己制定的信息安全管理标准太少，大多沿用国际标准。在标准的实施过程中，缺乏必要的国家监督管理机制和法律保护，致使有些标准企业或用户可以不执行，而执行过程中出现的问题得不到及时、妥善解决。

1.4.4　信息安全形势和事故分析

随着互联网的高速发展，互联网的相关应用已经渗透到千家万户，而互联网安全问题也进入了集中爆发时期。中国互联网络信息中心此前发布的报告显示，2012 年上半年，遭遇过病毒或木马攻击的网民为 2.17 亿，占网民总数的 44.7%；有过账号或密码被盗经历的网民达 1.21 亿；另有 8%的网民最近半年内在网上遇到过消费欺诈。在众多的互联网安全问题中，用户信息安全是最为敏感的问题，因为它直接关系到用户的隐私。

1．我国网络信息大规模泄露，受害网民过亿

一般来说，用户密码等信息被泄露主要有两个渠道，一是黑客盗取，二是网站主动销售获取利益。近期，据相关报道称，CSDN 网站被曝 600 多万用户的数据库信息被黑客公开，而随后天涯、开心网、人人网、新浪微博等网站也都相继被曝密码泄露，至此，密码被盗事件集中暴发，“今天你改密码了吗？”成为了当下最为流行的问候语。此次密码泄露事件是何种情况，目前并没有定论，但此次事件的暴发足以给整个互联网行业重重地敲响了警钟。

“泄密门”将网企漠视用户信息安全的短板彻底暴露出来，CSDN 像倒下的第一张多米诺骨牌，大量知名网站相继“沦陷”，拉开了我国互联网史上最大规模的用户信息泄露序幕，受害网民超过 1 亿，很多网友表示“改密码改到手软”。原以为自己在网上包得很密实，孰料在黑客眼中却是在“裸奔”。今天是网站信息，明天是银行信息，如何了得？

也许是不那么“显而易见”的缘故，人们往往十分在意交通安全、财产安全、人身安全，对信息安全的敏感度却要低得多。而事实是，信息安全同样十分重要。君不见，不仅有傻乎乎的局长拿微博当 QQ，公开约情人去酒店开房；更有那么多名人乐于当自己的“狗仔队”，走到哪里都将自己的行踪现场直播；

还有人将日记写在网上，事无巨细，无所不包。至于密码，就更是怎么方便怎么设，123456、111111、888888……易如反掌的破译，令心怀不轨的人想不动心都难。

针对多家网站发生的密码泄露事件，有专家提醒网民，尽量修改自己在网络上使用的密码，在上网的时候尽量不要提交敏感信息，以保证自己的信息安全。

用户信息频频泄露，对一个网民数量超过4亿、电子商务规模2012年有望超过6万亿元、网络实名制渐行渐近的国家来说，意味着什么？公众饱受垃圾短信、违法违规信息骚扰只是最低等级的危害，利用他人信息进行金融诈骗、洗黑钱以及盗取他人资金，则直接构成金融犯罪，扰乱金融秩序；而公众心理恐慌的生成，对电子商务、网络实名制、互联网的发展的损害更加深远。对此，管理层应有清醒的认识和警惕，思忖互联网安全的应对之策，防止用户信息泄露出现“破窗效应”，而不能止于“强烈谴责”与督促网站修补漏洞。

必须看到，公民个人信息的安全问题并非互联网的专利，回返到现实生活中的人们，亦从未跳脱信息泄露的阴霾。互联网与现实生活，已然不可分割。2008年，深圳市曾有4万名孕产妇信息被公开兜售，一度引来满城议论。几乎没有消停过的还包括，银行、医院、政府办事机构在内的诸多方面，都俨然成为公民个人信息无端被泄露的一个个丝毫不受控制的出口。

安全问题渗透于国民生活的几乎每一个层面，吃到嘴里的不求有益但奢无毒，行在路上只得寄望于上天庇佑，包括那些寄存于虚拟世界的个人信息，现在看来亦是岌岌可危。此番“泄密门”的漩涡不断扩大，只是再一次让人们打量和考问互联网信息安全的严峻性。

“道高一尺，魔高一丈。”任何信息安全技术都不可能永保无虞。与技术升级相比更关键的，是在法律上形成对网络犯罪的强力震慑。从目前我国的信息网络安全立法来看，开放性不高、兼容性不够、操作性不强等问题不同程度存在，“不得危害计算机信息系统的安全”等大而化之的内容较多，一些法规之间还存在交叉和冲突，与网络应用迅猛发展的形势不相适应。

我们只有把普及安全知识、树立安全观念、强化安全责任、提升安全技术、完善安全立法等措施结合起来，才能扎紧网络空间的篱笆，化解网络时代的“密码危机”，为下一步更大规模的电子商务、网络支付、网络实名制等奠定安全基础，让每个手握“网络存折”的人睡得安生。

2. 网络攻击日益趋利化

传统的黑客攻击网站、窃取信息通常只是为了炫耀技术、恶作剧或者仇视破坏，但随着互联网经济的发展，网络攻击的目的已转变为追求“经济利益”，并正在形成黑色产业链。根据国家计算机网络应急技术处理协调中心（CNCERT）近年来的监测表明，网络攻击者的攻击目标日益明确，针对不同网站和用户采用不同的攻击手段，且攻击行为趋利化表现明显：对政府类和管理相关类网站

主要采用篡改网页的攻击形式，以达到泄愤和炫耀的目的；对中小企业，尤其是以网络为核心业务的企业，采用有组织的分布式拒绝服务攻击等手段进行勒索；对于个人用户，攻击者更多的是通过窃取用户身份等手段，偷取该用户游戏账号、银行账号、密码等，窃取用户的私有财产，如利用网络钓鱼或域名劫持等手段对金融机构、网上交易、网络游戏等站点进行网络仿冒，在线盗用用户身份、密码或虚拟财产。2008 年上半年，我国大陆被植入木马的主机数量和被挂马网页数量双双大幅攀升，这是国内网络泄密、网银账号被窃事件频发的重要原因。

3. 病毒传播途径多样化

一是新计算机病毒的种类和数量呈几何级数增长，根据有关防毒机构监测，2008 年所收集到的新病毒样本几乎是 2007 年的 10 倍。二是病毒传播渠道发生了变化，2008 年所收集到的新病毒样本基本上是木马类的病毒，尤其网页挂马的方式占了 90%以上。这说明了现在病毒的制造和编写目的发生了根本性的改变，已经转向窃取一些重要的数据和信息，从而获取经济利益。三是 U 盘传播，现在网页挂马和 U 盘传播的病毒占了绝大部分，蠕虫类的病毒现在并不多见。

从病毒的发展趋势来看，病毒的制造技术在这几年没有发生根本性的改变，只是破坏的方式和目的有一些改变。病毒制造已经形成了流水线作业，实现了模块化，有更多的人参与到这个流水线中，所以病毒制造和传播的速度更快。还有一个趋势就是零日攻击，现在病毒制造和传播的主流方法就是利用漏洞，以前只有蠕虫是利用系统自身的漏洞来进行攻击的，但现在超过 60%的病毒是利用操作系统或应用软件的漏洞来进行传播的。病毒产业链的第一个环节就是漏洞，现在有人专门去搜集漏洞，某个软件的漏洞刚出来，就有人发现这个漏洞并转给另一批人对这个漏洞进行分析，制造相应的病毒和木马。这样，漏洞出来不到一天，攻击和威胁马上就出来了，所形成的零日攻击，对用户的威胁非常大。

4. 恶意代码层出不穷

新的恶意代码层出不穷也是安全形势日益严峻的主要原因之一。2008 年 1～6 月，CNCERT 共捕获不重复的恶意代码新样本总数 88 580 个，平均每天捕获 489 个，其中捕获次数位于前十位的恶意代码见表 1-1。

表 1-1　捕获次数位于前十位的恶意代码

排名	恶意代码名称
1	Virus.Win32.Virut.n
2	Net-Worm.Win32.Allap1e.b
3	Pom-Dialer.Win32.InstantAccess.dan
4	Trojan.Win32.Qhost.aei

续表

排名	恶意代码名称
5	Backdoor.Win32.VanBot.ax
6	Trojan-Downloader.VBS.Small.gg
7	Backdoor.Win32.SdBot.cp1
8	Net-Worm.Win32.Allaple.e
9	Virus.Win32.Sality.z
10	Backdoor.Win32.EggDrop.au

表 1-1 中的恶意代码主要利用微软系统的漏洞进行传播，并在感染的机器上留下后门程序，通过互联网中继聊天（IRC）、HTTP 等协议进行远程控制形成僵尸网络。黑客利用僵尸网络能够窃取被感染主机的系统信息，并控制被感染的机器发起新的扫描、DDoS、发送垃圾邮件或进行远程控制和网络欺诈活动等。

5. 垃圾信息依然泛滥

垃圾信息是指未经接收者同意而直接通过计算机、手机、固定电话等通信终端向接收者发送的各种电子信息。垃圾信息往往是那些毫无利用价值，甚至具有破坏性的信息。垃圾信息可能采用电子邮件、移动消息（短消息、多媒体消息等）、IP 多媒体或者其他形式传播。互联网的开放性和计算机信息易于扩散的特性也为垃圾信息的传播和泛滥提供了可乘之机。大量的商业信息、反动信息、色情信息以及带有欺骗性质的信息在没有得到用户许可的情况下发送到用户终端，不仅耗费了大量的网络资源和提高了用户的使用成本，还增加了社会的不稳定因素。近年来，越来越多的计算机病毒通过电子邮件、手机消息等方式传播，更是增加了垃圾信息的危害性，使我们在享受到信息化带来好处的同时又要面临垃圾信息的冲击。据统计，垃圾邮件占全球电子邮件通信量的 60%以上，每天约有 145 亿封垃圾邮件被发出，每年因此耗费 205 亿美元。

6. 网络融合带来新的安全

传统的电信网络，如固定电话网或 GSM 电话网，是一个封闭的环境，外部的攻击者很难进入系统进行攻击。因此在封闭性不被打破的条件下，传统电信网是安全的网络，是可信任的网络。随着我国电信网络向下一代网络的过渡和演进，这些封闭的环境将慢慢变得开放了。一方面，这种开放性使得外部的攻击者有了可乘之机；另一方面，由于传统电信网的封闭性，一些设计上的缺陷被封闭的环境掩盖起来，这些缺陷在相对开放的环境下就极有可能显现出来。例如，经过研究已经证实传统的固定电话网所采用的七号信令系统确实存在安全缺陷，难以在完全开放的环境中承受黑客的各种攻击。

随着三网融合和无线宽带进程的不断推进，为用户提供“永远在线”、尽可

能高速的数据速率以及动态的网络接入，同时也带来了一系列的安全问题，如漫游用户的机密性、接入控制和实体鉴权等问题。融合后的网络不但融合了各种网络的优点，也必然会将各种网络的缺点也带进融合后的网络中。而且，融合后的网络在能提供更多样化服务的同时也必将面临一系列新的安全缺陷，如网间信息的安全交互、密钥和证书的传输等都是很严重的问题。

总之，打赢网络信息安全保卫战，解决互联网信息安全问题需要多管齐下、合力为之。在相关法律法规的不断健全下，互联网企业方面应该大力投入到信息安全建设中，把保护用户信息真正当作自己的职责所在。而在用户方面，应该养成良好的网络使用习惯，能够明辨网络钓鱼等非法行为，共同营造一个健康安全的互联网环境。

1.4.5　信息安全对企业威胁分析

现在企业面临的安全挑战比以往任何时候都要严峻。随着渗透工具和漏洞利用攻击包逐渐商品化，安全旧患（如恶意软件等）又被赋予了新的力量。而我们的安全保卫战将是一场持久战，越来越多的员工与客户需要随时随地以多种方式进行网络通信，又更增加了安全战的复杂性。

更糟糕的是，不景气的经济环境让企业不得不消减对安全基础设施的投资。基于全球信息安全状态调查报告（对来自 130 多个国家的 7200 位 CEO、CIO、首席信息安全官、首席财务官以及其他负责企业 IT 和安全投资的执行人员的调查）的普华永道 2010 报告指出，安全项目范围减小以及项目部署推迟成为安全项目的成本控制的主要方法。

在过去 5 年中，认为“安全开支将增加”的受访者百分比显著下降（6 个百分点），超过 50%的受访者表示他们担心成本减少将更难实现安全保护，同时他们表示对企业资产的安全威胁正在增加。

由于威胁的增加和预算缩减的压力，IT 管理员的工作量也相应减少了，不仅包括抵御攻击的工作（他们现在应该已经非常熟悉工具和战略了），也包括向企业财务人员说明安全投资的工作。在很多公司、企业已经不愿意花太多资金在安全上了。现在首席信息安全官们不仅需要证明企业资产的安全性，还要提供数据说明这种安全性的价值。

业务领导与 IT 安全领导间协作加强是非常具有战略重要性的。在经济低迷时期，越来越少的资源被用于专门的安全功能上，然而业务领导在确定开展安全项目前，通常会要求周密且有说服力的计划。现在如果没有明确目标以及衡量是否成功的可靠方法，部署新的或者升级现有安全措施几乎不可能实现。

管理层的这些要求给安全人员带来新挑战。警报和报告形式的信息不仅能够确保安全设施有效运行，也能够记录安全设备的有效性。企业对管理、风险和合规的高度关注都驱使 IT 安全部门实现更大透明度，首先就需要部署精心设计的完整的且能够进行集中管理的安全方法，如防恶意软件、DLP（数据丢失

防御)、漏洞评估和软件漏洞修复等。管理威胁的能力以及结合报告与解决方案日志的能力变得越来越重要。

1. ERP 系统信息安全威胁

当前 ERP 系统是泛指针对物资资源管理、人力资源管理、财务资源管理、信息资源管理集成一体化的企业管理软件。ERP 系统实现了对整个企业供应链的管理，适应了企业在知识经济时代市场竞争的需要。鉴于 ERP 系统的巨大优势，目前绝大多数大型企业均实现了 ERP 系统的部署实施。然而，由于互联网上存在大量的网络攻击、木马、蠕虫等网络安全威胁，而 ERP 系统的正常运行依赖于大量的网络传输、数据处理和消息交互，这就阻碍了 ERP 系统的应用与实施。因此，研究 ERP 系统所面对的安全威胁并采取相应措施进行规避是一项非常重要的课题。

安全问题的产生是一个非常复杂的问题，包含了多种因素的相互作用。总结起来，企业 ERP 系统所面临的信息安全威胁主要包括来自以下几个方面的内容：

1）ERP 网络应用的威胁

来自网络层面的威胁主要来自远程访问企业内部系统所造成的信息泄露隐患。随着企业规模的不断扩展，对外的销售和物流网络也随之扩大，出差的业务员和某些客户经常需要在异地远程访问企业网络资源。为此，ERP 专门提供了 B/S 的访问模式，使得异地用户能够使用浏览器通过虚拟专用网络 VPN 访问公司内部资源。由于异地访问行为不受约束，泄密行为时有发生，有些价值较高的商业机密有可能流失，比如企业产品的底价、设计图样等等。

此外，内部网络的窃听行为也给 ERP 系统的安全使用造成威胁。ERP 系统应用时，其服务器端与客户端数据的传输，都是通过明文传输的，只需要在网络上安装一个监听软件，就可以全面地了解用户访问的内容，跳过客户端的权限设置，从而达到网络数据窃听的目的。

2）ERP 系统应用的威胁

如果 ERP 系统本身管理不当，也会存在数据泄露的危险。从 ERP 系统的角度出发，主要的安全威胁就是权限配置不当所造成的。这类威胁主要在于敏感数据缺乏分级管理机制，比如某个报表，只要有查看权限的都能够看到全部信息，并且能够导出，这就给敏感数据造成了很大的威胁。

此外，很多员工的终端系统密码设置较为简单，大多使用生日或者电话，有的甚至使用“12345”等简单数字作为密码，这类密码强度不高，容易被破解。

3）ERP 系统漏洞的威胁

ERP 系统的构建需要大量的软硬件系统，涉及网络传输、Web 浏览以及服务总线等多方面的技术，这些技术的实现需要大量的软件，软件不可避免存在一些已知或者未知的漏洞。黑客能够利用这些漏洞获取 ERP 服务器的权限，从而扰乱系统的正常运行，并窃取重要的商业机密。

ERP 系统的广泛应用是信息化推进和企业市场规模发展到一定阶段的产

物。如何在利用 ERP 带来的企业运营和管理便利的同时，尽可能避免安全威胁，是在 ERP 系统应用过程中需要详细考虑的问题。随着信息安全技术的不断发展，不断有新的威胁会出现，也需要 ERP 系统进一步提高安全意识，防范可能的网络攻击行为。

2. 内部信息泄露成威胁企业安全的主流

当今的企业面临更复杂的信息安全问题。与个人用户相比，公司中存在大量的高质量数据。大多数公司都开放了社交网络页面，存在更多可接入点，员工的移动性仍在增加，各种新、旧安全问题摆在企业面前。在新的安全防御面前，拉拢内部工程师、敏感数据的利益诱惑等等比创建新的恶意软件要容易得多。2010 的 Verizon 数据泄露调查报告显示内部原因造成的数据泄露较上一年增加了两倍多，达到了 46%，内部威胁会成为攻击主流。

安全领域首先会面临内部威胁持续增加的挑战。在今近几年里，行业中的各大事件和新的发现影响了企业的安全性和运营。

为企业解决内部数据安全问题，最理想的做法是从企业业务风险大小出发，告之企业一旦数据泄露对其业务影响有多大，这种影响绝不是只对其 IT 层面。如果企业的图样和源代码等核心数据泄露，企业整体都必须为其承担风险，而风险程度对于每个企业是各不相同的。例如，某厂商的一款芯片的相关核心技术提前泄露，由于一款芯片的生命周期是 18 个月，那么泄露一款芯片对企业就不仅仅是半年到一年的影响，而意味着未来 18 个月企业都很难翻身。这对企业来说不是简单的几十万的损失，而是几百万甚至更多的无法预估的损失。所以要把数据泄露放在企业运营层面看待，它不仅仅保护企业内部的一些流程，不是对企业 IT 架构有多重要，而是对企业有多重要。数据安全不单单为一个部门，而是为企业运营解决问题。

信息安全另一方面是社会学工程，其行为主体是人，制定人性化、规范化的安全管理制度也是抵御泄露的重要部分，所以业界素来有“三分技术，七分管理”的说法，一个完整的企业内控安全系统应是技术手段和管理制度相结合的产物，它可以有效地弥补某些无法用技术手段实现的安全漏洞。

3. 黑客盗取信息牟取暴利 ，成企业网络安全最大威胁

利用“黑客”技术侵入企业内网、破坏他人网站，窃取数据信息借以非法牟利，这种网络犯罪已渐成产业。对于企业和整个社会来说，黑客网络犯罪将造成极大危害。这就要求企业必须对网络安全给予足够重视，更需要相关部门在立法、技术上给予保障，多管齐下，方能保证网络安全。

1）黑客盗取信息愈发“市场化”

社交网站以及一些审查不严的应用程序商店受到黑客的攻击越来越猛烈，黑客们惯用伎俩是，在社交网站页面上附加仿冒的病毒扫描。比如，突然间弹出一个窗口说，“你的系统可能受到感染，但我们会为你做一个免费的扫描”。

还有一个更高级一点的版本，那就是让这个窗口无法关闭。在用户们为病毒扫描这一诈骗手段头痛时，黑客又把目标瞄向了商业信息。该网站使用一个虚假的解码器，把链接指向另一个发布有视频的网页。如果要播放这段视频就得下载这个假的解码器，而它实际上是一个专为盗取商业信息而设计的恶意软件。

2）黑客出手动机多来自利益诱惑

有知情人士透露，黑客的每日收入最高已经达到 12000 元，这样的诱惑会导致越来越多的 IT 人才转向黑客一行，而最终导致的结果就是使企业蒙受苦难。

在香港，愈来愈多网上黑客盗取信息转售图利。有调查发现，现在新增恶意程序数量，超越过去 10 年总和，亚太区约 75%的受访企业曾遭黑客入侵，被盗取知识产权、客户信用卡数据及客户个人身份。

2008 年，被告人汤某采用黑客手段非法侵入北京市仁爱教育研究所的网站，致使该网站无法正常访问，并以帮助恢复网站为条件，向仁爱教育研究所索要人民币 5000 元。

2009 年底，包括“温柔”系列木马的全国最大制售木马病毒案在江苏宣判。该案涉及 16 个省市，涉案金额高达 3000 多万元，引起了社会的广泛关注。

路透社曾报道，西班牙警方已经破获了一个计算机黑客集团，这些黑客曾通过一个病毒控制了超过 1300 万台计算机，以盗取信用卡和其他有价值的数据。“这是迄今发现的最大规模‘僵尸网络’。”西班牙警方网络犯罪部门负责人贝罗卡尔说，世界上估计存在 4000～6000 个“僵尸网络”。协助西班牙警方破获此案的加拿大防务情报公司和西班牙熊猫安全公司掌握的情况显示，被感染的计算机分布于全球 190 个国家和地区，全球前 1000 家最大企业中有一半以上企业的计算机曾被这一病毒感染，另有超过 40 家主要银行的计算机遭侵入。

4．社交网站成企业信息安全最大威胁之一

开心网、人人网、微博，这些社交网站在中国兴起的时间虽然还不长，却已经以不可阻挡的势头成为写字楼里白领的最爱，没事更新一下心情、发布一点感想，分享几张照片，抱怨几句生活，是众多企业职员上班时间的重要消遣。然而，社交网络吸引的不只是普通的网民，一些网络犯罪分子也同样将目光锁定在这里。

研究表明，社交网站用户更容易遭遇财产损失、信息被盗和恶意软件感染等安全威胁，其严重性甚至超过用户自己的想象。

近日，卡巴斯基实验室发布了“全球 IT 安全风险调查”，调查显示，社交网站已经被视为企业信息安全最大的威胁之一，仅次于点对点文件分享（P2P）。

在卡巴斯基调查的所有样本公司中，有 53%的公司完全屏蔽了对社交网络的访问，另有 19%的公司对员工的这类行为进行了限制。卡巴斯基实验室全球研发和分析小组总监 Costin Raiu 说：“社交网络通常被视为消耗时间的行为，并且还可能会造成潜在的恶意软件攻击，对公司机密数据造成威胁。”

社交网站最常见的攻击形式是“钓鱼”。犯罪分子以用户的身份出现，然后

向其好友发送包含恶意程序的网站，该用户好友一旦登录到这个网站，就可能遭受不同程度的损失，此前曾经在中国用户中引起轰动的新浪微博集体中毒事件正属此类。由于当时这一针对微博的恶意攻击尚属首次，也并未植入可记录用户密码的木马，因此没有造成严重的后果。但社交网站中潜藏的危机和网络威胁藉此传播的超快速度已经初露端倪，未来，这一点很可能被网络犯罪分子加以利用，并得以窥探企业内部的机密数据。

5. 钓鱼攻击成为企业主要安全威胁

成功利用钓鱼邮件对安全企业（如 Oak Ridge 和 RSA 等）造成的数据泄露攻击为我们敲响了警钟，一些专家嗤之以鼻的低技术含量攻击方法也可能造成严重威胁。

美国能源部研究实验室 Oak Ridge 近日宣布发现在其网络中存在数据窃取恶意软件程序后，已经关闭了所有互联网访问和电子邮件服务。根据该实验室表示，这次数据泄露事故源于一封发送给 570 名员工的钓鱼攻击邮件。这封电子邮件伪装成该实验室的人力资源部门的通知，当一些员工点击嵌入在电子邮件中的链接后，恶意程序就被下载到他们的计算机中。这个恶意程序利用了微软 IE 软件中未修复的漏洞，并且目的是搜寻和窃取该实验室的技术信息，该实验室的工程师们正在努力研制世界上最快的超级计算机。Oak Ridge 实验室的官方发言人形容这次攻击与安全供应商 RSA 遭受的攻击非常类似。

RSA 数据泄露事故导致了 RSA 公司的 SecurID 双因素认证技术信息的被窃。而 Epsilon 发生的数据泄露事故也被怀疑是有针对性的钓鱼攻击行为，这次事故是有史以来涉及最多电子邮件地址的事故。

分析家表示，攻击者能够利用低技术含量、假冒电子邮件的方法来渗透进入这些受到良好保护的企业表明了有针对性的钓鱼攻击日益成熟，并且存在这样的趋势，企业认为单靠教育员工就能够缓解这个问题。“这并不让我感到惊讶，”安全公司 Invincea 公司创始人 Anup Ghosh 表示，“几乎每个公开的和发表声明的高级持续性攻击都是通过钓鱼邮件开始的。”

事实上，现在这类邮件似乎成为攻击者非法进入企业网络的首选方法，他表示。“你需要做的就是设立一个电子邮件目标，你只需要通过几次点击就能够在企业内部建立几个存在点，”Ghosh 表示，“如果你企业有 1000 名员工，并且你教育他们不能打开不可信任的附件，还是会有那么几个人会打开。这并不是训练可以解决的问题。”

让问题更严重的就是钓鱼攻击越来越复杂，分析师指出，越来越多的有组织的攻击团队开始使用精心设计的电子邮件来针对高层管理人员以及企业内部他们想要攻击的员工。在很多情况下，钓鱼邮件都是个性化的、本地化的，并且设计得好像是来自可信任来源一样。

Ghosh 表示，他就收到过类似的邮件。邮件发送到他的个人邮箱，看起来是一个好朋友发过来的邮件，包含一个能够打开朋友的女儿生日派对照片的链

接。邮件甚至还包含朋友女儿的名字。邮件被标记为红色，但是 Ghosh 在点击链接后才发现红色标记。他说：“随便看一眼就已经能够说服我去点击链接。”

Spire Security 公司的分析师 Pete Lindstrom 表示，“最近很多攻击都是使用某种形式的钓鱼攻击，这个十分令人担忧，我们总是很容易在一些安全基础环节掉链子。”

公司必须定期记录和监测网络是否存在这种钓鱼攻击造成的数据泄露，他表示。在钓鱼攻击中，企业必须更注重响应和遏制，而不仅仅是预防，分析师 Rich Mogull 表示，在这种攻击中，企业常常面对的是拥有丰富资源、耐心和资金的对手。通常情况下，这样的对手都愿意不断尝试直到他们攻入系统网络。“几乎不可能阻止这样的人。”

同样重要的是，企业需要广泛地监控内部网络以确保数据没有泄露出去。

6．安全软件和服务并不安全

在计算机出现病毒，或者希望计算机可以抵御未知的安全风险时，我们常常想到的就是安全软件和服务。这些产品和服务似乎让我们感觉自己得到了保护。然而，近日国外的一项调查报告却揭示，实际上，我们的安全软件和服务也并非是“安全”的!你愿意接受这个残酷的事实么?

近日 Veracode 发布的最新报告显示，测试的大部分安全软件和安全服务软件的安全评分都“难以置信”的低，也就是所有商业软件中超过 65%的安全软件和服务安全状况并不理想。

Veracode 公司最新发布的软件安全状态报告显示客户支持软件比安全产品以及服务更糟糕，其中 82%的应用程序评分都非常低，而相对的，安全软件和安全服务软件则是 72%。

Veracode 扫描的所有商业软件中有 66%的软件在第一次安全扫描中都得到了“无法令人接受”的低分，安全产品和服务软件的低分数是最令人震惊的。“这真的让我们很惊讶，”Veracode 公司产品营销副总裁 Sam King 表示，该公司对超过 4800 个应用程序进行了扫描分析，“这也解释了最近在 RSA、HBGary 和 Comodo 发生的数据泄露事故的原因，攻击者开始瞄准安全公司以及其他垂直行业，这里给我们的教训是：你无法想象的是，安全供应商可能都不安全。”

第2章 企业风险与信息安全

企业的风险系统是围绕着不断改善这个想法建立的，包括合规遵从规划。如果一切都顺利的话，企业建立和管理规划来确保他们完全地遵从策略、流程、规划、法律、法规等等。但是企业管理者意识到，尽管他们的出发点很好，事情有时也不会按计划进行，必须防患于未然。一般地，企业风险管理与内部控制的工作中，60%在业务管理控制上，而40%是在IT控制上的。所以，企业在合规管理方面也要求企业必须落实到对IT的有效管理控制上来。本章从企业合规风险、企业数据泄露风险以及企业业务连续性风险三个层面进行分析，以进一步帮助企业认识信息安全风险，说明打赢企业信息安全保卫战的重要性。

2.1 企业合规风险

企业合规经营是指企业的经营行为应符合和遵从相关法律规范。经营合规风险就是分析企业在合规方面是否符合法律要求，包括安全策略和技术合规性的检查、系统审查等相关事项。合规风险对应的安全合规性管理属于信息安全管理领域的一部分。

2.1.1 从企业合规风险看IT管理风险

美国萨班斯法案（SOX）的产生源自于上市公司操作的不规范和公司丑闻的披露，它要求上市公司针对产生财务交易的所有作业流程，都做到能见度、透明度、控制、通信、风险管理和欺诈防范，且这些流程必须详细记录到可追查交易源头的地步。因此，SOX法案明确提出了所有上市公司都必须加强和建立有效的内部控制框架，以确保上市公司遵守证券法律和提高公司披露信息的准确性和可靠性。

2008年6月，我国财政部、证监会、银监会、保监会及审计署委联合发布了被称为“中国版萨班斯法案”的《企业内部控制基本规范》，此规范于2009年7月起在上市企业中实施。其中，该规范第37条规定：“企业应当建立重大风险预警机制和突发事件应急处理机制，明确风险预警标准，对可能发生的重

大风险或突发事件，制定应急预案、明确责任人员、规范处置程序，确保突发事件得到及时妥善处理。”

与我国的《企业内部控制基本规范》第 37 条规定相比较，在“美国版萨班斯法案”中也有类似条款，比如第 404 条款规定：企业必须了解那些可能影响财务报告流程的风险，并必须要实施恰当地控制以阻止财务违法行为。此外，SOX 法案第 404 条款还要求，企业需建立一个基础设施，以确保所有的记录和数据不会被毁灭、丢失、未经授权的变更和错误的使用。由于 IT 和财务报告的关联性，故 IT 也需要加强控制以达到 SOX 法案的合规要求。因此，上市公司在建立符合《萨班斯—奥克斯利法案》要求的企业风险管理与内部控制的工作中，60%在财务控制上，而 40%是在 IT 控制上的。所以，SOX 法案在合规方面也要求企业必须落实到对 IT 的有效管理控制上来。

遵从 SOX 法案，要求上市公司的高管和业务、管理、技术等各个部门都要积极应对。首先，对公司高管而言，要求他们必须清楚其对于公司财务报告、信息披露和内部控制报告的责任，不遵从 SOX 法案所面临的法律后果和证券市场的风险，掌握公司各个部门遵循 SOX 法案进行内部控制的措施和执行情况，降低遵从 SOX 法案所花费的内外部成本等。其次，受 SOX 法案影响最大的是财务部门，对于财务部门尤其是 CFO 而言，要求能够提供真实、准确、可靠的财务信息，按时完成季度及年度的公司财务报告，建立和维护内部控制结构和程序，与外部审计人员有效配合，并有责任减少遵循 SOX 法案所产生的内部及外部审计成本。

此外，还要看到，SOX 法案涉及所有影响财务报表生成的其他业务部门，其中影响较大的是 IT 部门。SOX 法案有一些条款是与 IT 直接相关的，包括 302 条款对财务报告的提供，404 条款内控报告的提供，409 条款实时披露材料的变更，802 条款为审计和评审员保留相关的记录等。对 IT 部门而言，遵循 SOX 法案，要求 IT 部门要支持公司高管、财务和内外部审计人员的需求，以确保影响财务报表的业务流程、应用和信息基础设施的完整性、可用性和可审计性，保证内控报告和内控程序的完成，并能够对外部审计需求作出积极响应。

为遵从 SOX 法案，保证会计账务、财务报告、流程、财务应用和底层 IT 基础结构的完整性、可用性和准确性，要求 IT 在三方面有所准备：

一是优化财务流程，完善财务应用系统。在财务应用的基础上，要实现财务数据整合和统计分析，引进全面预算管理、KPI 绩效管理、财务预警等模块，保证企业提供准确、完整、实时、真实的财务报告。

二是建立内部控制体系并引入内控管理信息系统。SOX 法案要求企业高管加强对内控程序和内控报告的责任，要求 CEO 和 CFO 能够证明年度和季度财务报告没有差错和遗漏现象，要求企业记录并检查企业的内部控制情况，揭露任何“严重弱点”，要求企业高层能够判断与业务过程相关的风险，以及这些风险对公司财务报告可能产生的影响。达到上述要求的核心内容首先是建立公司内部控制体系，美国“反对虚假财务报告委员会”的 COSO 内部控制框架包括

控制环境、风险评估、控制活动、信息与沟通和监督五个要素，强调建立一系列的管理体制，加强公司的内部控制。IT 是 COSO 实施的关键，应建立起遵从 SOX 法案的企业内控管理信息系统。

内控管理信息系统至少应实现下述功能：能够创建和记录企业内部业务流程，使公司的 CEO、CFO、员工和审计人员能够实时识别、分配、测试并监视内部控制与流程，确保业务流程根据内控标准执行。一旦系统发现任何违反行为，将向适当人员自动报警。能够收集并监视控制信息，使管理人员快速查看流程、组织、控制和风险的实时状态，提示管理人员注意控制目标是否实现。为了帮助企业更好地了解和跟踪风险，内控管理信息系统为企业建立一个能够与企业的每项业务过程相关联的风险库。一旦认识出潜在风险，内部控制管理系统能够允许企业设计控制以降低风险。

三是加强 IT 控制。SOX 法案要求企业的内控活动，不论是人还是信息系统的操作流程都必须明白地定义并保存相关记录，对审计过程也有存档的要求。因此，对影响财务报告的信息系统的 IT 控制，也是 SOX 法案内部控制的核心组成之一。这就要求 IT 完善治理机制，进行 IT 内部控制和信息系统审计，以保证达到 SOX 法案对 IT 的基本要求。国际上已经形成一些较为完整的 IT 治理的规范，如 ITIL（信息技术基础架构库）、COBIT（信息和相关技术的控制目标）、BS 7799（信息安全管理标准）等。其中，COBIT 是信息系统审计与控制协会提出的 IT 治理的控制框架。ITSM（IT 服务管理）的标准 ITIL 则与 COBIT 紧密一致，通过 IT 服务管理流程与产品，能够实现 IT 的规范化管理，记录和控制 IT 的基本信息，包括对网络、硬件、网页、应用、防火墙、信息系统访问控制权限、访问密码等信息，保证财务报告的底层 IT 基础结构的业务持续，帮助公司更有效监督和管理 IT 风险。

2.1.2　从 SOX 合规性看我国 IT 内控规范

1．为什么内控合规必须以 IT 为突破口

无论是美国的 SOX 法案还是我国的《企业内部控制基本规范》涉及的东西都比较多，在这里我们主要关注的是 IT 内控方面的内容。在很多公司内部，财务报告流程是由 IT 系统驱动的。无论是 ERP 系统还是其他系统，都与财务交易中的开始、批准、记录、处理和报告等活动紧密集成。比如财务报告保存在财务系统里，财务系统的数据从业务系统来，业务系统的数据也存放在相关的数据库里，数据库又是保存在服务器上，服务器还可能跟网络互联。因此，在财务信息操作上只要有一丝的漏洞，都可能是被 IT 系统出卖的。因此，合规的问题不再只是 CEO、CFO 的职责，IT 部门在这方面也将渐渐承担主角。简单的说，IT 是保证财务报告内部控制有效性的基础。

虽然，我国的《企业内部控制基本规范》要求企业实现的内控是以战略为导向的全面内控，但该规范包括的范围相当广泛，仅内控这项内容就包括企业

层面、业务流程、IT 一般控制与 IT 应用控制。其中涉及企业运营的方方面面，从企业战略管理、财务管理、供应链管理、生产管理到人力资源管理、OA 办公管理等。由于所有的业务都可能产生数据，而如何确保数据的及时收集、准确与完整性都离不开 IT 系统的支撑。因此，如何把 IT 内控与企业内控管理统一起来，是合规《企业内部控制基本规范》的一个关键点。也就是说，在内控合规方面，IT 就是一个最佳的突破口。

2．借鉴 SOX 合规对 IT 内控的要求

SOX 法案对 IT 内控要求主要有两个方面：一方面是 IT 应用控制（IT Application Control），是因为大多数上市公司在一定程度上都依赖 IT 系统来运作业务，IT 系统对业务流程的控制作用非常大，因此必须对业务流程所依赖的 IT 系统进行某些控制，其中特别是针对支持财务报告的特定 IT 应用。另一方面是 IT 一般控制（IT Generally Control），是因为上市公司必然有一个完整的 IT 系统做支撑，所以对于支撑公司运作的 IT 基础技术架构平台，必须进行有效管理控制。其中主要是针对基本的 IT 基础设施控制，包括物理和逻辑网络安全、数据库管理、系统开发、变更控制、灾难恢复等。

SOX 法案是一部典型的法律文件，它既不是管理手册，也不是行动指南。它只规定了上市公司在整体或业务层面上必须达到的要求，却没有指明上市公司应该如何达到法案规定的水平。比如 SOX 法案要求企业的 IT 内控必须有效，但落实到具体 IT 控制方面 SOX 法案则完全没有给出任何的指导意见。例如，上市公司需要什么样的 IT 控制，如何进行 IT 控制和 IT 内控效力如何评估等全都不在 SOX 法案范围之内。

但根据上市公司内控需求和 SOX 法案的合规性管理描述，IT 部门的主要职责和活动应该包括：

（1）深入了解公司的内控项目和财务汇报流程；

（2）确定与内控活动或财务汇报流程相对应的 IT 系统；

（3）分析和辨别这些 IT 系统带来的风险，并对此进行监控以保证控制措施的长期效力；

（4）将控制措施文档化和 IT 化，并进行测试；

（5）及时地对 IT 控制进行必要的升级和变更，以配合公司内控或财务汇报流程的变化；

（6）作为一个重要的职能部门，IT 部门应该全程参与公司 SOX 法案合规管理项目。

2.1.3 安全合规性管理

合规性（compliance），在 ISO/IEC 17799 里就有明确要求。ISO/IEC 17799

在合规性方面规定了“符合法律要求；安全策略和技术合规性的检查；系统审查相关事项”等要求。对应的安全合规性管理属于信息安全管理领域的一部分，那时的安全合规性管理主要包括识别适用的法律法规，保护个人信息的隐私；使用合法的、正版的系统软件与应用软件；加强计算机安全审计，保障技术和安全策略的合规性等工作。随着萨班斯法案（SOX）的出台和广泛使用，安全合规性管理开始逐渐受到电信运营商、证券业、银行业、跨国公司等各方人士的追捧。

随着信息安全设施的逐渐完善，企业对安全管理提出了更高的要求，越来越多的企业高层意识到控制安全风险的重要性，开始重视安全合规性管理。数据丢失将会对业务造成巨大的影响，有时公司的管理层还将承担法律责任。在数据失窃方面做得非常成功的公司，都通过提高合规性效率，推动网络运营和治理，尤其是在日常控制、安全控制以及过程方面。如何提高合规性的审核效率，特别是针对自动化控制和流程的监控技术，是当今安全技术发展的趋势。完善的合规性管理方案可以将安全管理人员从耗时、耗力的审核任务中解放出来，使安全防范工作流程化，这正是各类大型企业的强烈愿望。企业从单纯采购安全产品或安全集成项目演化到一体化的集中信息安全管理的趋势日益明显，将安全管理、系统管理、存储管理与合规政策融为一体形成企业信息安全管理框架是大势所趋。

2.2　企业数据泄密风险

本节针对企业业务数据泄密风险、企业的需求、保护核心资产等方面分析，并从安全评估、风险分析、风险治理三个层面进行论述。

2.2.1　数据安全评估

要清楚认识到企业自身的数据安全现状，就必须有一套清晰的评估方法。这里可以提供三点评估方法供大家参考：

数据保密意识是否具备？

数据保密措施是否缺乏？

数据保密制度是否健全？

在我们看来，评估一家企业的数据安全现状，必须以人为本。企业领导是否有数据保密意识？员工是否能遵守保密制度？这都是关键。企业领导和员工具备良好的保密意识，辅之健全措施和制度，能大大提升企业核心资产的信息安全。当然，这与企业的信息化程度以及数据是否以电子文档形式存在也有很大关系。

2.2.2 数据安全风险分析

1. 数据不同的表现形式、不同的运行机理将产生不同的风险点

敏感数据的表现形式多样化。企业内使用的数据可以归纳为五类：业务类（客户资料、财务报表、交易数据、分析统计数据）、行政类（市场宣传计划、采购成本、合同定单、物流信息、管理制度等）、机要类（公文、统计数据、机要文件、军事情报、军事地图）、科研类（调查报告、咨询报告、招投标文件、专利、客户资产、价格）、设计类（设计图、设计方案、策划文案等）。现今企业的敏感数据存在的形式再也不仅仅是文档，而是在业务系统中流转的数据、在服务器中共享的数据、在个人存储中保存的数据、在设计软件中展现的数据、在邮件中正文信息及附件中涵带的数据、交付第三方的信息等等。

2. 敏感数据的风险差异化

保密数据以不同的应用方式，呈现出不同的应用形态。任何一个企业内部无论它的机构怎么样，均可以把它分成五个基本环境：

（1）内部核心数据部门，像研发部、设计部等，风险高度集中；

（2）内部的办公区域，如财务、销售、行政机构等，仅需要适当的防范；

（3）服务器区域，数据的存在方式以及访问的权限需明确；

（4）经常移动办公的人员，安全并须兼顾便捷；

（5）数据需要交换到的外部机构，数据的严格可控。为了保证数据不被恶意获取，这些都是应该注意的非常重要的应用场景。

3. 数据安全风险分析

敏感数据在其产生、存储、应用、交换等不同环节的应用过程中，均存在泄密风险。因此，数据风险的评估、系统整合、体系的建立与合理的使用都将是考虑因素。

2.2.3 数据安全风险治理

面对前面提到的种种风险，企业该如何避开这些风险？如何将企业面临的数据泄露风险降到最低？这就是涉及对风险的管控和治理。

要做好企业风险治理，首先必须明确目标，这个目标就是将企业信息泄露风险降到可接受水平。之所以这样讲，是因为保证信息的绝对安全是不存在的。其次就是要分析企业信息安全盲点，包括技术上和制度上的，然后逐一消除这些盲点。

那么如何将企业的信息泄露风险降低到可接受水平，并消除企业可能存在的信息安全管控盲点？

针对核心的敏感数据区，往往也是数据生成的核心地带。数据的产生目的是为了被使用。例如，一张设计图样，可能需要打印、传输给上级、交付生产、

生产出来的产品的测试等等，这些数据会通过不同的途径、以各种形态流转在多个业务系统环节中。这样，在方案设计时，就要保证数据的整个生命周期的安全：

（1）要保证数据产生的环境安全，除了提供数据泄密风险防护的基本产品组件以外，还需要考虑与管理的联动，如边界防护的防火墙、统一审计的日志管理、第三方的身份认证等的联动。

（2）保证数据的使用可控，每个数据本身将有所属身份及使用权限，谁可以使用、如何使用、使用的周期等，不仅仅要有严格的控制，更需要有科学的管理设置，如我们增加了审批流程以及不同审批结果的响应方式。

（3）保证数据必要的通道安全，如需要交付给第三方的数据，如何交付？交付后如何受控？需要与数据使用的各种业务系统联动管理，我们提供应用保护系统，确保数据可以准确并受控地到达数据使用者手中。

（4）在现代化的管理企业中，企业的文化、保密的思想、管理的制度都应是防护体系的一环，需要设置对应的合理、高可执行的管理体系。

根据用户关注的数据风险差异、应用场景的不同而提供多元化的解决方案，在方案中所有体系既独立，又可以互相组合形成更完整的解决方案，同时也能够提供优良的扩展性，为集团或者跨行业单位提供基于不同应用的数据保密解决方案。

2.3 从企业风险分析认识信息安全风险

所有的风险系统是围绕着不断改善这个想法建立的，包括合规遵从规划。如果一切都顺利的话，企业建立和管理规划来确保他们完全地遵从策略、流程、规划、法律、法规等等。但是业务管理部门意识到，尽管他们的出发点很好，事情有时也不会按计划进行。在成熟的组织内，对于发生了什么错误以及为什么发生的了解，为组织提供了完善他们计划的绝好机会。

为了从影响企业业务的突发事件中吸取教训，公司必须能够开诚布公地讨论关键的问题，“为什么那件事会发生”和“对于那件事情我们该做什么”。这个关于常规性流程失败的谈话足以让人感到尴尬，也许会损失一些金钱或是给一些顾客带来不便。当涉及导致业务中断的信息安全问题时，紧张程度往往呈指数级增长。

数据安全与其他大多数业务风险略有不同，安全和合规团队正努力管理以达到“零事件发生”（换句话说，数据泄露是不可接受的结果并且绝对不能发生）。理智上我们知道那（数据泄露）是可能的，但是当事情发生时人们往往想尽可能快地处理掉它并且继续前行。同样的规则也会适用于其他所有业务故障，但是如果合规规划参与者没有从他们的错误中吸取教训，这个规划永远不会变得更好。对于组织的风险管理和合规规划来说，没有比同一件事情发生两次更难堪的了。

坦率地讲，许多组织对发生的故障保持缄默，以避免尴尬、职责或法律责任。那些明显成熟的组织（以及管理团队）意识到，如果没有从错误中学习到的数据和教训，那就不是真正意义上的管理风险，而只是管理事件。

一旦辨识出突发事件，合规遵从团队必须先回答以下四个关键的问题，从而回到一个稳定状态。

（1）发生了什么事情？这要求公正地分析到底发生了什么问题。

（2）这件事情意味着什么？接下来从财务、业务、名誉和监管暴露方面分析对组织的可能影响。在初期进行估计，然后随着更多的信息可用时进行调整。

（3）这个事件还在发生么？是否数据仍然在泄露？如果是这样的话，现在需要做什么来补救问题？

（4）必须做什么来让一切回到正规？需要采取什么恢复步骤来解决客户数据泄露，通知监管机构、管理媒体的询问等等？

这样，事情应该明朗了，这个过程基本上集中于事故响应和破坏控制，但是到目前为止这些措施并不能告诉我们为什么事件会发生，以及它如何体现了组织的风险概况。一旦事件处理完成，然后就可以开始真正有价值的工作了（很不幸的是，一些组织在这里戛然而止）。随后的问题就是：

（1）与故障有关的控制问题：

① 控制缺失？完全不存在控制措施。

② 控制不充分？问题的风险或是结果被低估或是误解。

③ 控制是多余的？预期的损失少于合适的控制成本。

④ 控制执行失败？正确地设计了控制措施，但就是没有遵守。

（2）是否有到位的机制来充分地识别事件并对其作出响应？

（3）假定有关于事件的新信息、需要的效果和恢复尝试，这会如何影响组织理解它的风险和相关控制措施的？对风险概况的新认识是否影响特定的合规遵从要求？

（4）价值百万元的问题：我们有什么需要改变？

当分析完成、弄明白需要改变什么（如果有的话）后，行动起来！如果在经历了所有这些工作后没人接棒继续前行（无论是推理或体制上的障碍），没有比这更会扼杀人们对分析过程的重视了。

从长远来看，另一个关键的因素就是记录、记录、再记录。没有记录的话，组织永远无法彻底从这些分析中获得体制上的教训。任何不止一次地经历了故障的组织，需要仔细查看他们记录事件的能力，并真正从中学习。

最后，通过从这些详细的分析中排除责任因素，组织有望仔细地审视到位的控制，并且诚实地评估他们是否做好充足的准备继续前行。但是（这一点很重要），如果事实上是某个特定的人造成了问题，首先应该衡量这个人应该提高什么或是应该做什么，这就是组织如何来建立问责制度。

有些经理最初可能不太愿意和太多人进行这种类型的分析，这个想法是对的。涉及的主要负责人必须参与进来，以进行充分的分析、记录结果并作出恰当的运作改变。随着时间的推移，人们会发现这些练习对于风险和合规遵从规划是富有成效和巩固的。

第3章

信息安全管理内涵

信息安全管理究竟对企业而言意味着什么？企业如何打赢一场信息安全保卫战？为此，本章先从信息安全的定义出发，分别从四个层面讨论企业信息安全及其实施内涵，其次综述了企业信息安全建设的四个阶段，最后论述企业信息安全建设的目的意义。

3.1 信息安全概述

随着全球范围内数据泄露、黑客攻击等安全事件不断出现，信息安全工作的重要性已为人们所接受，很多企业目前都将信息安全工作提到了战略性的高度。然而，企业信息安全究竟要做什么？要关注哪些方面？如何来落实？这些问题一直困扰着企业的管理者，为此，本节先从信息安全的定义出发，讨论企业信息安全及其实施内涵。

3.1.1 传统信息安全的定义

“信息安全”曾经仅是学术界所关心的术语，就像五六十年前“计算机”被称为“电算机”那样仅被学术界所了解一样。现在，“信息安全”因各种原因已经像公众词汇那样被世人所熟知，尽管尚不能与“计算机”这个词汇的知名度相比，但也已经具有广泛的普及性了。问题的关键在于人们对“计算机”的理解不会有什么太大的偏差，而对“信息安全”的理解则各式各样。种种偏差主要来自于从不同的角度来看信息安全，因此出现了“计算机安全”、“网络安全”、“信息内容安全”之类的提法，也出现了“机密性”、“真实性”、“完整性”、“可用性”、“不可否认性”等描述方式。

关于信息安全的定义，以下是一些有代表性的定义方式：

（1）国内学者给出的定义是：“信息安全保密内容分为实体安全、运行安全、数据安全和管理安全四个方面。”

（2）我国相关立法给出的定义是：“保障计算机及其相关的和配套的设备、设施（网络）的安全，运行环境的安全，保障信息安全，保障计算机功能的正

常发挥，以维护计算机信息系统的安全。”这里面涉及了物理安全、运行安全与信息安全三个层面。

（3）英国 BS 7799 信息安全管理标准给出的定义是：“信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。”

（4）美国国家安全局信息保障主任给出的定义是：“因为术语‘信息安全’一直仅表示信息的机密性，在国防部我们用‘信息保障’来描述信息安全，也叫‘IA’。它包含五种安全服务，包括机密性、完整性、可用性、真实性和不可抵赖性。”

（5）国际标准化委员会给出的定义是：“为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。”这里面既包含了几个层面的概念，其中计算机硬件可以看作是物理层面，软件可以看作是运行层面，再就是数据层面；又包含了属性的概念，其中破坏涉及的是可用性，更改涉及的是完整性，显露涉及的是机密性。

从信息安全的作用层面来看，人们首先关心的是计算机与网络的设备硬件自身安全，就是信息系统硬件的稳定性运行状态，称为“物理安全”；其次人们关心的是计算机与网络设备运行过程中的系统安全，就是信息系统软件的稳定性运行状态，称为“运行安全”；当讨论信息自身的安全问题时，涉及的就是狭义的“信息安全”问题，包括信息系统中所加工存储和网络中所传递的数据的泄露、仿冒、篡改以及抵赖过程所涉及的安全问题，称为“数据安全”。因此，从信息安全作用点来看问题，可以称之为信息安全的层次模型，这也是国内学者普遍认同的定义方式，如图 3-1 所示。

从信息安全的基本属性来看，机密性就是对抗对手的被动攻击，保证信息不泄露给未经授权的人，或者即便数据被截获，其所表达的信息也不被非授权者所理解；完整性就是对抗对手主动攻击，防止信息被未经授权的篡改；可用性就是确保信息及信息系统能够为授权使用者所正常使用。这三个重要的基本属性被国外学者称为“信息安全金三角”（CIA，Confidentiality-Integrity-Availability），如图 3-2 所示。



图 3-1　一种信息安全的层次模型

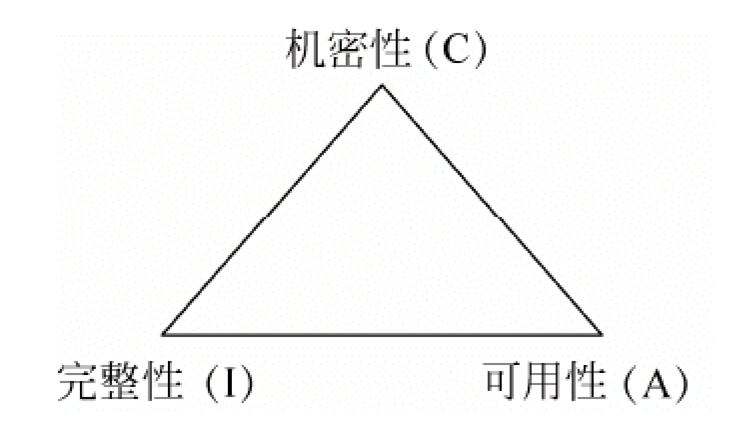


图 3-2　信息安全金三角模型

3.1.2　信息安全技术与信息安全管理

信息安全技术是实现信息安全产品的技术基础，信息安全产品是实现组织

信息安全的系统设备。信息安全管理是通过维护信息的机密性、完整性和可用性等，来管理和保护信息资产的一项体制，是对信息安全保障进行指导、规范和管理的一系列活动和过程。

单纯考虑技术，只能作出功能强大的信息安全产品，并不能对组织机构内部信息的安全保障提供直接的支持。单纯考虑管理，缺少技术产品的支撑，就不能很好保证信息安全规章制度的很好实施，因为许多实现规章制度的信息安全管理手段方法、活动与过程需要好的安全产品支撑。

3.1.3　当代信息安全的新内容

从信息安全的作用层次来看，前面已经介绍了人们所关注的三个层面，即物理安全层、运行安全层以及数据安全层。但是，还有两个层面尚未在同一个框架之下给出清晰地描述。一个是关于信息内容的安全问题，一个是关于信息对抗的问题，这两个层面的安全问题也是业界普遍关心的问题。所不同的是，内容安全更被文化、宣传界人士所关注；而信息对抗则更被电子对抗研究领域的人士所关注。

信息内容安全的问题已经深刻地展现在现实社会面前，主要表现在有害信息利用互联网所提供的自由流动的环境肆意扩散，其信息内容或者像脚本病毒那样给接收的信息系统带来破坏性的后果，或者像垃圾邮件那样给人们带来烦恼，或者像谣言那样给社会大众带来困惑，成为社会不稳定因素。但是，就技术层面而言，信息内容安全技术的表现形式是对信息流动的选择控制能力，换句话说，表现出来的是对数据流动的攻击特性。

信息对抗严格上说是信息谋略范畴的内容，是讨论如何从多个角度或侧面来获得信息并分析信息，或者在信息无法隐藏的前提下，通过增加更多的无用信息来扰乱获取者的视线，以掩藏真实信息所反映的含义。从本质上来看，信息对抗是在信息熵的保护或打击层面上讨论问题，也就是围绕着信息的利用来进行对抗。

由此可见，机密性、真实性、可控性、可用性这四个基本属性实际上就是信息安全的四个核心属性，可以反映出信息安全的基本概貌。相对信息安全金三角而言，可称之为信息安全四要素，简称 CACA，如图 3-3 所示。

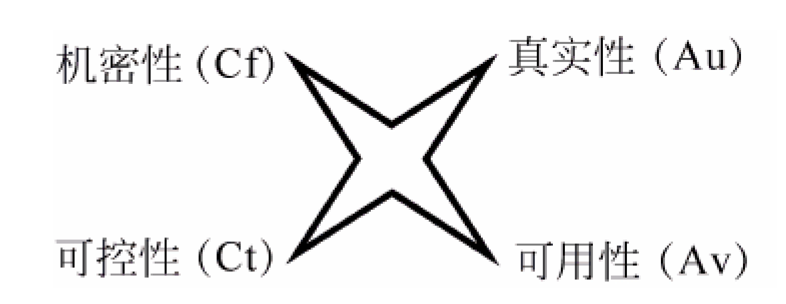


图 3-3　信息安全四要素

根据这一思路，重新定义信息安全的概念如下：信息安全是对信息系统、信息与信息的利用的固有属性（即“序”）攻击与保护的过程。它围绕着信息系

统、信息及信息熵的机密性、真实性、可控性、可用性这四个核心安全属性，具体反映在物理安全、运行安全、数据安全、内容安全、信息对抗五个层面上。

综合信息安全的层次性特性与安全属性特性，可以形成一个信息安全概念的经纬线，如表 3-1 所示。

表 3-1 信息安全概念的经纬线

	机密性	真实性	可控性	可用性
物理安全	√	√		√
运行安全		√	√	√
数据安全	√	√		√
内容安全	√	√	√	√
信息对抗	√	√		

信息安全专家方滨兴院士在深入分析和继承了传统信息安全的定义前提下，根据当前国际信息安全的发展现状，给出了信息安全四要素，并重新概括和界定了信息安全的内涵和外延。方院士提出了五个“四”的法则，第一个“四”是从四个层面考虑信息安全的问题，即物理层、运行层、数据层、内容层；第二个“四”是安全的四个基本属性，即可用性、机密性、可鉴别性、可控性；第三个“四”是保障信息安全的四个目标，即要做安全的网络、可信的网络、可靠的网络、可控的网络；第四个“四”是从四个确保的源头来保障信息安全，即软件确保、系统确保、服务确保、使命确保；第五个“四”是保障网络主权的四项基本权利，即独立权、平等权、自卫权、管辖权。

1. 信息安全四要素

物理安全表现在能量供给上，运行安全主要表现在代码攻击上，数据安全主要是面对数据攻击，内容安全是从内部的安全来考虑的。

1）物理安全

物理安全层面主要考虑的因素有：

（1）安全网络的抗打击性如何，未来网络的设备冗余性如何，是否可热备份、容灾？网络的可生存性如何，是否可剪裁运行，可降级运行？

（2）网络设备损毁后的自恢复能力如何，网络的去中心化程度如何？传统的中心依存度尽量低，避免形成安全瓶颈口。

（3）网络自组织的程度如何？网络的重组能力如何？

（4）网络设备是否能被攻击致瘫？

2）运行安全

运行安全的问题主要表现在以下几个方面：

（1）网络是否能够承受拒绝服务攻击，是否能够承受住资源的过度消耗？

（2）网络是否能够被非授权控制？要具有防止网络运行系统的安全漏洞被利用的能力。

（3）核心设备是否能够被攻击？要具有持续地提供核心功能的能力。

（4）网络路由是否会被劫持，是否会形成错误的路由？要具有防止网络路径被非法重定向与错误路由污染的能力。

（5）网络寻址服务是否能够被终止服务？防止寻址服务体系被瘫痪。

3）数据安全

关于数据安全问题，主要考虑的因素有：

（1）网络的运行状态是否能够被欺骗？防止网络状态被伪造，防止网络路由信息被欺骗。

（2）网络传输通道是否能保证数据的隐私？要具有防止信息被泄露与被非授权扩散的能力。

（3）网络传输通道是否能够保证数据不被篡改？要具有信息不被篡改的能力。

（4）网络身份信息是否能够被仿冒？要具有身份鉴别的能力。

（5）网络信息传输具有防抵赖的能力。

4）内容安全

内容安全考虑的因素有：

（1）网络信息是否能够被监测？具有对网络信息进行标签的能力，或者具有授权认知网络信息的能力，再或具有授权发现隐藏信息的能力。

（2）网络信息是否能够被控管？要具有授权过滤指定信息的能力，要具有限制指定信息发布的能力。

（3）网络信息是否能够不被非授权扩散？就是要具有数字版权保护的能力。

（4）网络系统是否具有被局部隔离的功能？要具有切割非授权介入的子网的能力。

2. 信息安全的四个属性

信息安全应关注的四个属性包括可用性、机密性、可控性、可鉴别性。可用性要注意被攻击的问题，机密性要注意高效的问题，可控性要注意自由的问题，可鉴别性就是隐私的问题。

1）可用性

（1）要保证网络的可用性，需采取必要的措施，使网络始终处于可提供服务的状态，从而使得授权用户可以随时获得服务。网络应该具备一些可靠性，要保证网络出现故障的概率极小。

（2）网络应该具备稳定性，保证网络不出现可被用户感知的问题。网络还应该具备可生存性，保证网络在极端条件下仍然能够提供核心服务，尽管其服务质量在下降。

（3）网络应具备可维护性，主要指在线维护。

2）机密性

（1）要保证网络的机密性就是要确保网络传播的信息不被非授权者所获知，

并要保证网络信息的实用性，需采取措施，使得网络加密信息唯一依赖于对应的密钥。

（2）要保证网络信息不会被捕获、复制与扩散，需采取屏蔽、隔离措施，防止非授权截获与传播信息。

（3）要保证网络不能被非法获得，需采取访问控制措施，防止非授权访问信息。

（4）要保证网络信息不被非法认知，需采取加密措施。

3）可控性

要保证网络的可控性，主要的目标是采取措施，使得网络始终处于授权掌控状态：

（1）具备可追溯性，保证网络传播的源头与目的是可追溯的。

（2）具备可记账性（可确定性），保证网络传播的所有状态均可被记录并保存。

（3）具备可审计性，保证网络传播的所有状态具有相关责任主体。

（4）具备可过滤性，保证网络信息是可被理解的。网络信息传播的源头与目标是可被理解的，指定信息是可被过滤的。

4）可鉴别性

（1）要保证网络的可鉴别性，主要是保证与网络传播相关的信息其真实性是可以被鉴别的。

（2）网络信息应该具备完整性，保证网络信息的任何篡改都能够被鉴别出来。

（3）网络的传输主体与客体的身份应具备真实性，保证网络信息传播的发放方与接收方的身份是可鉴别的，符合预知的身份。

3. 信息安全应保障的四个目标

首先要保证是一个安全的网络，保护网络不被致瘫，网络上的攻击可被有效遏制，网络上的用户不被攻击所困扰；其次要保证是一个可信的网络，确保对网络传输的行为人及传输的信息可被鉴别，其可信程度可被判定；然后要保证是一个可靠的网络，确保能够提供有效的服务，不因随即故障而失效；最后要保证是一个可控的网络。

（1）从前提假定来说，安全是一个恶人的假定，攻击是必须的；可信是一个好人的假定，只要是好人就不会有攻击；可靠是上帝的假定，是随机的；可控是一个监管人的假定，服从约定的形式，攻击是来自缺陷的概念。做一个比喻，安全就像养猛兽，我们把它当作宠物，肯定不会真的跟它一起睡觉，风险太大了，把它用链子拴起来，可信就像养宠物狗，可靠就像养一个牲畜，可控就像养孩子。行为类比一下，安全就像一个人要闯红灯，可信就像绿灯行，可靠就像黄灯行，可控就像红灯停。应用原则：安全就像在监狱的状态，可信就像在办公室的状态，可靠就像猪圈，可控就像居家状态。

（2）从立足点来看，安全是事先保护，可信是事后打击，可靠是经济平衡，可控是规则管制。

（3）从应用点来看，安全是未知身份，可信是已知身份，可靠是随机因素，可控是自有系统。

（4）从追求目标来看，安全追求的是不受伤害的状态，可信是证明它确是一个好人，可靠是保证尽量不受损失或者损失不能太大，可控是掌控一切。

（5）从手段来说，安全是以降低风险为目的，可信是依赖历史，可靠是投保机制，可控是监控。

（6）从风险来看，安全方面就是资源消耗太大，可信最怕意外变节，可靠是概率损失，可控是失控了。

4. 信息安全的四个确保

首先从源头做起，做软件确保，其次是系统确保，然后是服务确保，最后是使命确保。整个的安全确保就是从源头一直到目标，目标是为了保护使用者。

1）软件确保

（1）保证网络协议是符合预期的，要求网络协议的实现在需求、设计、编码、验证等环节都通过证明或检验。

（2）保证网络协议不存在可利用的漏洞，要求网络协议具有自保护特性，即便出现安全漏洞也不会被恶意利用。

（3）保证网络协议的实现环节是符合规程的，要设计协议实现规程，保证协议的软件实现是符合规程的。

（4）保证网络协议软件的可信性。

2）系统确保

（1）保证网络系统的功能是可预期的，要给出证据以证明网络系统的形式化方法起到了极其重要的作用，要提高网络系统没有漏洞的确信程度，要具有网络系统的自防护能力，使得无论在系统生命周期的任意时刻，即便漏洞作为系统的一部分有意或无意设计或插入的，也不能够被利用起来形成攻击。

（2）保证网络系统在装配之后是可信的，可信的软件还需要可信的接口，以保证系统的可信性，因为网络系统是一个系统工程。

3）服务确保

（1）保证网络系统能够提供符合要求的服务性能。

（2）保证通信服务提供商能够利用策略和过程确保所提供的服务满足预先定义的服务质量。

（3）保证网络系统能够提供有保证的服务。

（4）具备故障和事件管理、性能管理、探测监视、服务质量管理、网络和服务测试、网络流量管理、客户管理、服务等级协议监视等能力。

4）使命确保

（1）保证网络系统的自适应性能够适应用户的需求，尽管网络本身没有受

到攻击，也要具备弹性变化的能力，以降低风险。

（2）保证网络系统能够提供有效的服务，无论网络系统有多复杂，规模有多大，要保证始终处于用户能够得到服务的状态。

（3）要求网络系统处于全世界周期工程状态，要保证网络系统设计、生产、测试与运行方面服从需求工程的要求，持续支持在线更新。

5. 网络主权

网络主权的内涵就是基本权、独立权、平等权、自卫权和管辖权。独立权是指本国的网络可以独立运行，无需受制于他国；平等权是指网络之间的互联互通是以平等协商的方式来进行的，不受管辖制约等。

1）独立权

对于独立权而言，就是要确定一个国家网络可以独立存在。现有的互联网由于根域名解析体制的缘故，不能够独立存在，因此受制于美国，除非根域名解析归属一个类似于联合国的国际组织管理，域名解析系统的管理权就可以被理解为各国出让了本国对该系统的管理权而集中在指定的国际组织，同时该国际组织在章程中被各国所认可，各国对该国际组织的运行具有同等的权利。未来网络可以考虑类似于路由机制来建立分布式名字服务系统，各国的名字服务系统不受制于任何国家以及任何国际组织，可以独立存在，类似于国际贸易可以遵循国际策略，也可以多边协商，还可以双边协商。

2）平等权

确保各国的网络之间可以以平等的方式进行互联互通，要像民航航线一样相互对等地开辟互联互通的航线，互联互通不能成为单方受惠的建设模式。目前的互联网的国际介入受制于大的国际运营商，如 Sprint 公司，因其在国际上具有重要的地位，致使互联网规模小的国家在介入时往往会受到不平等的待遇，

还要确保各国对网络系统具有平等的管理权，要保证一个国家对本国互联网的管理不会伤及到其他国家。现有的互联网相互依赖过度，互联网强势国家所制定的政策可能波及其接受服务的国家。

3）自卫权

网域空间已经受到各国重视，众所周知美国的三大战略：核战略、太空战略、网域战略，目前的五大战场已经是领海、领土、领空、领天、领网络了，已经要保护网络了，现在要做的系统要确保网络系统可以处于自我保护之下，而不是依赖于他国进行保护，不应该有境外系统被攻击致使本国网络瘫痪的情况发生。本国要是拥有对网络攻击的自卫能力的话，一定要拥有隔离能力。

4）管辖权

首先要拥有对本国网络系统的管理能力，网络的接入要能够实施市场准入机制，非授权子网应该不能够接入到网络中，要具备发现非授权接入网络的能力，对网络的接入要能够事后终止，对于不服从管理的业务应该具有停止服务的能力。现有的系统不具有这样的能力，如谷歌退出中国基本上不影响向中国

所提供的服务。国际上有一个河床与河水的概念，水是没有主权的概念，物理社会中国家对河床拥有主权，尽管河水来自上游国家，但上游国家不能输出被污染的河水。

3.1.4　信息安全框架及其实施内涵

从上一节的论述不难看出，当代信息安全定义在企业信息安全中的使用还存在以下几个问题，需要进行进一步改进。

（1）概念含糊不清，且没有给出实施的可用参考：只是列出了信息安全需要关注的协议层面、系统单元和牵涉到的几个安全属性；而在安全属性中，流量机密性和机密性本来就是同一回事，所采用的技术也是大同小异，并没有给出企业在信息安全的保障实施过程中的任何可行性建议和手段。

（2）忽略了管理安全：该框架只强调技术，而忽略了管理在企业信息安全保障中的重要作用和地位。所谓“三分技术，七分管理”，没有管理的技术难以落到实处，缺乏管理的指导性，盲目的使用技术也是不合理的。

为了根据企业的自身特点来制定可行的企业信息安全框架，我们可以回顾一下信息安全定义。结合企业在信息安全工作的特点，将其中的“信息对抗”改进为“管理安全”，这主要是由于以下两个重要原因：

其一是企业的信息安全工作主要是“防”，以防为主，立足自身，基本上不会采取信息对抗的方式来还击外部黑客和不法用户，所以称之为企业信息安全保卫战。

其二是企业的信息安全工作很大一部分在于满足外部对企业的审核要求，企业对自身员工、资源等的管理要求，这就依赖于管理安全，他们需要参考和遵循许多业界成熟的标准和制度，比如 ISO/IEC 27001、萨班斯法案等。

因此，企业要打赢一场信息安全保卫战，就要构建一个信息安全框架。其本质是：企业信息安全从技术角度来看是对信息与信息系统的固有属性的攻击与保护的过程。它围绕着信息系统、信息自身及信息利用的机密性、真实性、完整性、可控性、可用性、不可抵赖性这六个核心安全属性，具体反映在物理安全、运行安全、数据安全、内容安全、管理安全五个层面上，如图 3-4 所示。

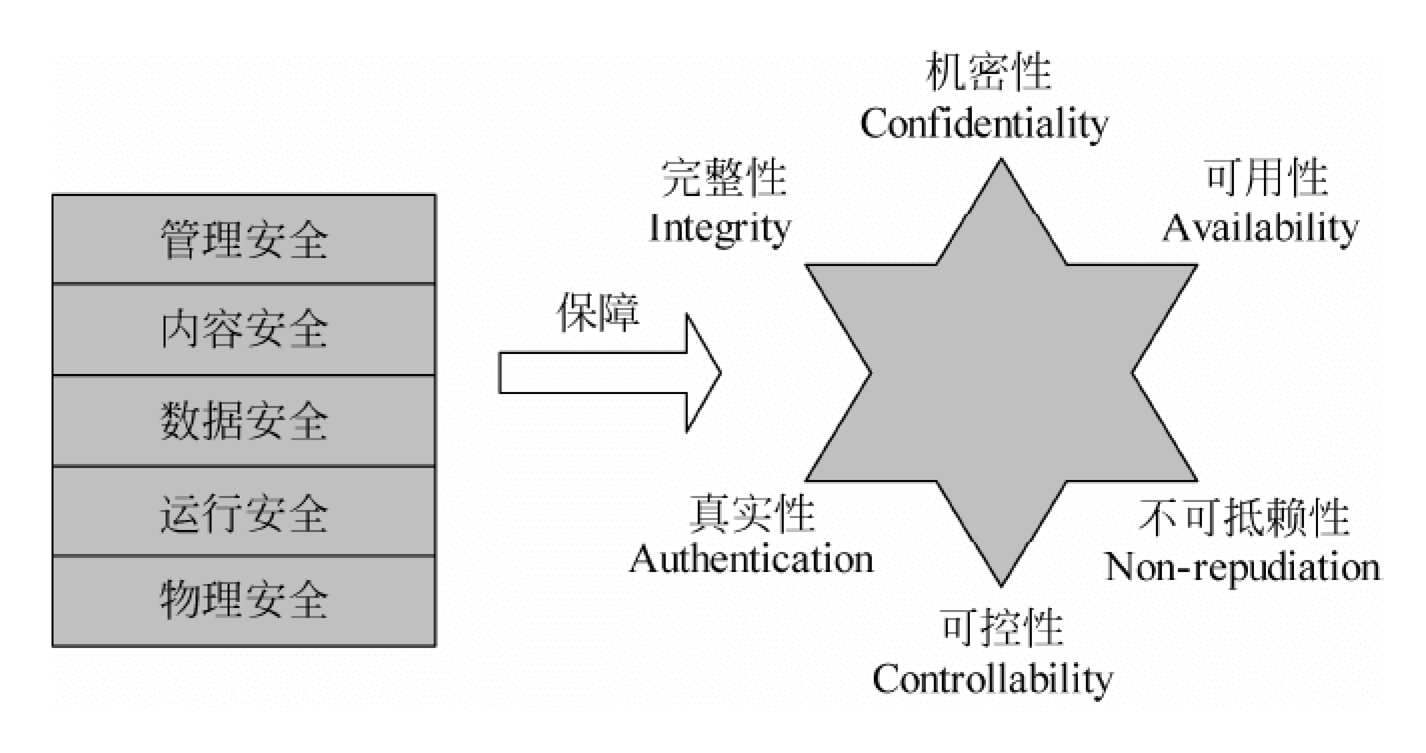


图 3-4　企业信息安全框架

3.2 信息安全建设阶段分析

参照信息安全建设的经验和根据企业信息安全建设的实际情况，可以从安全制度和安全技术两个维度把企业安全建设阶段分为四种类型或四个阶段，分别是被动型企业（事件导向阶段）、技术型企业（技术导向阶段）、制度型企业（流程导向阶段）和成熟型企业（风险导向阶段），如图 3-5 所示。

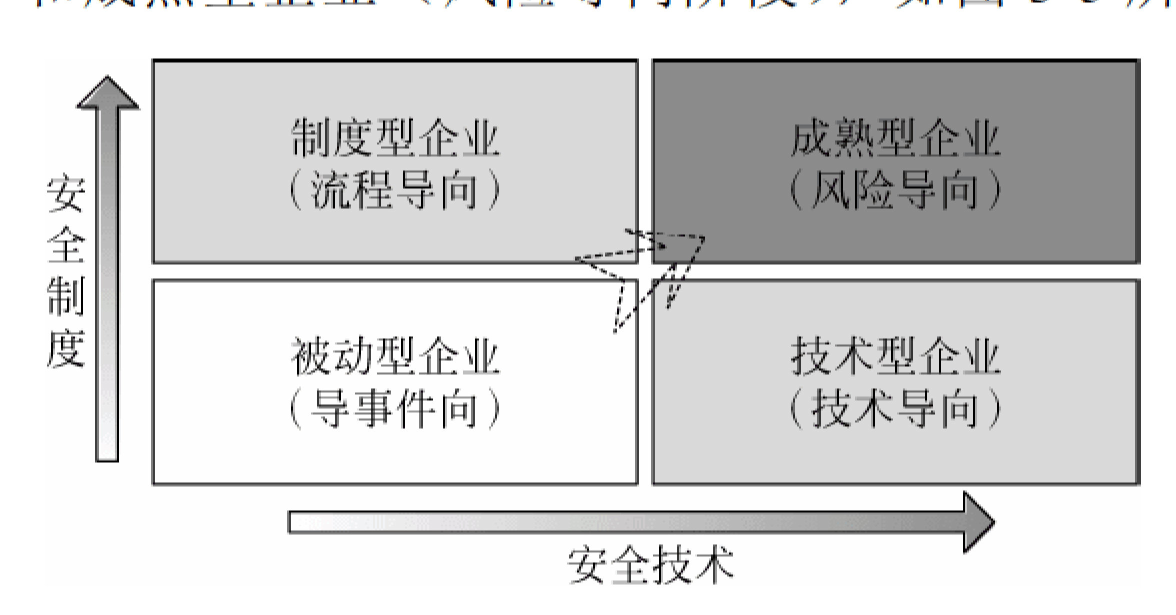


图 3-5 企业信息安全建设的四个阶段

下面就四个阶段的特点分别给予说明。

1. 被动型企业（事件导向阶段）的主要特点

（1）事件、故障发生以后再采取相应的补救措施；
（2）不注重 IT 的安全管理；
（3）无计划中的信息安全预算；
（4）使用基本的用户名、密码管理；
（5）部署了基本的安全工具；
（6）每年信息安全投资预算占整个 IT 预算的份额非常低。

这个阶段属于信息安全建设的初级阶段，目前大多数中小企业都属于这一阶段。

2. 技术型企业（技术导向阶段）的主要特点

（1）强调并依赖 IT 的安全技术；
（2）部署了各种领先的安全工具；
（3）每年安全经费预算投入在 IT 投资中开始被重点考虑，数量有较大增加；
（4）尚未建立正式的安全组织，有一定的安全策略、标准和流程；
（5）员工安全意识普遍比较薄弱。

这一阶段属于大量技术投入阶段。

3. 制度型企业（流程导向阶段）的主要特点

（1）强调安全管理的重要性；
（2）每年信息安全经费预算有所增加；

（3）开始对信息资产进行分类；
（4）建立了正式的安全组织；
（5）拥有完善的安全策略、标准和流程；
（6）部署了基本的安全工具，但安全制度和流程无法有效落实。

4．成熟型企业（风险导向阶段）的主要特点

（1）强调 IT 的安全管理和安全技术的平衡；
（2）建立集成且统一的安全体系管理架构、技术架构；
（3）拥有基于国际标准的完善的安全策略、标准和流程；
（4）建立了强健有力的安全系统；
（5）应急响应机制完善且定制演练；
（6）预防为主、防治结合、内外兼修。

通过对目前企业信息安全建设的现状分析，希望我们可以把握自己企业的信息安全建设现状，在信息安全的建设和管理过程中树立正确的观念，通过参照信息安全建设相关的方法论和最佳实践，走出一条简洁和有效的建设之路。本书的后面章节将进一步论述。

3.3　信息安全建设目的意义

信息安全建设对企业的安全管理工作和企业的发展意义重大。首先，将提高员工信息安全意识，提升企业信息安全管理的水平，增强组织抵御灾难性事件的能力，是企业信息化建设中的重要环节，必将大大提高信息管理工作的安全性和可靠性，使其更好地服务于企业的业务发展；其次，通过信息安全的建设，可有效提高对信息安全风险的管控能力，通过与等级保护、风险评估等工作接续起来，使得信息安全管理更加科学有效；最后，信息安全管理体系的建立将使得企业的管理水平与国际先进水平接轨，从而成为企业向国际化发展与合作的有力支撑。

参照信息安全管理模型，按照先进的信息安全管理标准建立全面规划、明确目的、正确部署、组织完整的信息安全管理体系，达到动态的、系统的、全员参与的、制度化的、以预防为主的信息安全管理方式，实现用最低的成本保障信息安全合理水平，从而保证业务的有效性与连续性。组织建立、实施与保持信息安全管理体系产生的作用主要有以下几点：

（1）强化员工的信息安全意识，规范组织信息安全行为；
（2）对组织的关键信息资产进行全面系统的保护，维持竞争优势；
（3）在信息系统受到侵袭时，确保业务持续开展并将损失降到最低程度；
（4）使组织的合作伙伴和客户对组织充满信心；
（5）如果通过体系认证，表明体系符合标准，证明组织有能力保障重要信息，提高组织的知名度与信任度；
（6）促使管理层坚持贯彻信息安全保障体系。

第4章

信息安全发展与相关标准

本章主要论述信息安全发展历程与相关信息安全标准体系。首先综述了信息安全发展的四个阶段；其次论述了信息安全管理类标准的提出与发展；最后分别对 ISO/IEC 2700X 系列标准、信息安全管理实施与指导类标准、信息安全测评标准、国家标准以及国家信息安全等级保护体系进行了概要的论述，以便读者对国内外标准体系有一个系统了解和认知，为读者后续深入学习和查阅相关标准提供一个基础。

4.1 信息安全发展

4.1.1 信息安全发展历程

信息安全发展大致经历了四个时期，如图 4-1 所示。第一个时期是通信安全时期，其主要标志是 1949 年香农发表的《保密通信的信息理论》。在这个时期通信技术还不发达，计算机只是零散地位于不同的地点，信息系统的安全仅限于保证计算机的物理安全以及通过密码（主要是序列密码）解决通信安全的保密问题。把计算机安置在相对安全的地点，不允许非授权用户接近，就基本

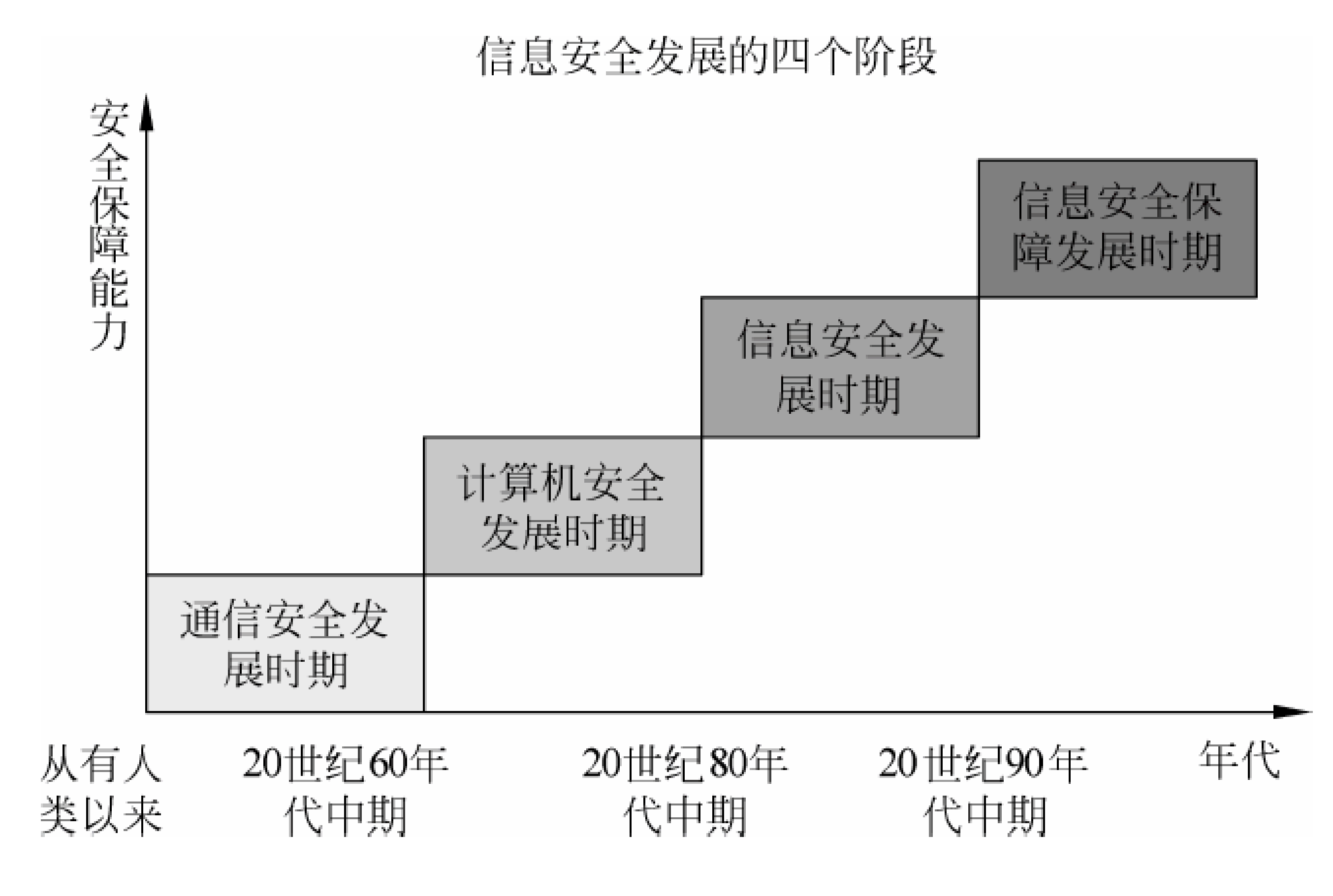


图 4-1 信息安全发展的四个阶段

可以保证数据的安全性了。这个时期的安全性是指信息的保密性，对安全理论和技术的研究也仅限于密码学。这一阶段的信息安全可以简称为通信安全，它侧重于保证数据在从一地传送到另一地时的安全性。

第二个时期是计算机安全时期（20 世纪 70～80 年代），其主要标志是《可信计算机评估准则》（TCSEC）。在 20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软、硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，数据的传输已经可以通过计算机网络来完成。这时候的信息已经分成静态信息和动态信息。人们对安全的关注已经逐渐扩展为以保密性、完整性和可用性为目标的信息安全阶段，主要保证动态信息在传输过程中不被窃取，即使窃取了也不能读出正确的信息；还要保证数据在传输过程中不被篡改，让读取信息的人能够看到正确无误的信息。

1977 年美国国家标准局（NBS）公布的国家数据加密标准（DES）和 1983 年美国国防部公布的可信计算机系统评估标准（Trusted Computer System Evaluation Criteria，TCSEC，俗称橘皮书，1985 年再版）标志着解决计算机信息系统保密性问题的研究和应用迈上了历史的新台阶。

第三个时期是在 20 世纪 90 年代兴起的网络时代。从 20 世纪 90 年代开始，由于互联网技术的飞速发展，信息无论是企业内部还是外部都得到了极大的开放，而由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经从传统的保密性、完整性和可用性三个原则衍生为诸如可控性、抗抵赖性、真实性等其他的原则和目标。

第四个时期是进入 21 世纪的信息安全保障时期，其主要标志是《信息保障技术框架》（IATF）。如果说对信息的保护，主要还是处于从传统安全理念到信息化安全理念的转变过程中，那么面向业务的安全保障，就完全是从信息化的角度来考虑信息的安全了。体系性的安全保障理念，不仅是关注系统的漏洞，而且是从业务的生命周期着手，对业务流程进行分析，找出流程中的关键控制点，从安全事件出现的前、中、后三个阶段进行安全保障。面向业务的安全保障不是只建立防护屏障，而是建立一个“深度防御体系”，通过更多的技术手段把安全管理与技术防护联系起来，不再是被动地保护自己，而是主动地防御攻击。也就是说，面向业务的安全防护已经从被动走向主动，安全保障理念从风险承受模式走向安全保障模式。信息安全阶段也转化为从整体角度考虑其体系建设的信息安全保障时代。

4.1.2 信息安全发展趋势

信息安全发展主要呈现四大趋势。总的来说，现在的信息安全技术是基于网络的安全技术，这是未来信息安全技术发展的重要方向。

1. 可信化

可信化趋势是指从传统计算机安全理念过渡到以可信计算理念为核心的计

算机安全。近年来计算机安全问题愈演愈烈，传统安全理念很难有所突破，人们试图利用可信计算的理念来解决计算机安全问题，其主要思想是在硬件平台上引入安全芯片，从而将部分或整个计算平台变为“可信”的计算平台。目前还有很多问题需要研究和探索，如基于 TCP 的访问控制、安全操作系统、安全中间件、安全应用等。

2．网络化

由网络应用和普及引发的技术和应用模式的变革，正在进一步推动信息安全关键技术的创新发展，并诱发新技术和应用模式的出现。例如，安全中间件、安全管理与安全监控都是网络化发展带来的必然的发展方向；网络病毒和垃圾信息防范都是网络化带来的一些安全性问题；网络可生存性、网络信任都是要继续研究的领域……

3．标准化

安全技术也要走向国际，也要走向应用，我国政府、产业界、学术界等必将更加高度重视信息安全标准的研究与制定工作的进一步深化和细化，如密码算法类标准、安全认证与授权类标准、安全评估类标准、系统与网络类安全标准、安全管理类标准等。

4．集成化

集成化趋势即从单一功能的信息安全技术与产品，向多种功能融于某一个产品，或者是几个功能相结合的集成化的产品方向发展，不再以单一的形式出现，否则也不利于产品的推广和应用。安全产品呈硬件化/芯片化发展趋势，这将带来更高的安全度与更高的运算速率，也需要发展更灵活的安全芯片的实现技术，特别是密码芯片的物理防护机制。

4.2 信息安全管理标准的提出与发展

信息安全标准的发展大体经历了“零星追加时期”和“标准化时期”两个阶段，20 世纪 90 年代中期可以看作这两个阶段的分界。信息安全实践发展的三个标志阶段，一是技术浪潮，二是管理浪潮，三是制度浪潮。没有完善的信息安全标准，信息化建设中的产品、系统和工程就不能实现安全的互联、互通、互操作，就不能形成信息安全产业，就不能构造出一个自主可控的信息安全保障体系。

1993 年，英国贸易工业部制定了世界上第一个信息安全管理体系（ISMS）实施标准，即 BS 7799-1：1995《信息安全管理实施规则》，其提供了一套综合的、由信息安全最佳惯例组成的实施细则，其目的是作为确定企业信息系统所

需控制范围的参考基准，适用于大、中、小型组织。

由于 BS 7799-1：1995《信息安全管理实施规则》采用指导和建议的方式编写，因而不宜作为认证标准使用。

1998 年，为了适应第三方认证的需求，英国又制定了世界上第一个 ISMS 认证标准 BS 7799-2：1998《信息安全管理体系规范》，它规定了 ISMS 要求与信息安全控制要求，可以作为对一个组织的全面或部分 ISMS 进行评审认证的标准。

BS 7799-1：1995《信息安全管理实施规则》主要是给负责开发的人员作为参考文档使用，从而在机构内部实施和维护信息安全。

BS 7799-2：1998《信息安全管理体系规范》详细说明了建立、实施和维护信息安全管理体系的要求，指出实施组织需要通过风险评估来鉴定最适宜的控制对象，并根据自己的需求采取适当的安全控制。

BS 7799 的目的：为信息安全管理提供建议，供那些在其机构中负有安全责任的人使用，它旨在为一个机构提供用来制定安全标准、实施有效安全管理的通用要素，并不涉及“怎么做”的细节，它是制定一个机构自己标准的出发点。

BS 7799-1 与 BS 7799-2 经过修订，在 1999 年重新发布，并考虑了信息处理技术与通信领域应用的快速发展，也非常强调商务，涉及信息安全的责任。2000 年 12 月，BS 7799-1：1999《信息安全管理实施细则》通过国际标准化组织 ISO 的认可，正式成为国际标准——ISO/IEC 17799：2000《信息技术—信息安全管理实施细则》。

2002 年 9 月 5 日，BS 7799-2：2002 正式发布，该版标准主要在结构上做了修订，引入 PDCA（Plan-Do-Check-Action）管理模型，建立了与 ISO 9001、ISO 4001 和 OHSAS 18000 等管理体系标准相同的结构和运行模式。

2005 年，BS 7799-2：2002 正式转换为国际标准 ISO/IEC 27001：2005。BS 7799-2 从 1998 年发布后，在世界范围内得到广泛的认可，目前已经有 40 多个国家和地区开展信息安全管理体系的认证。

4.3　ISO/IEC 2700X 系列国际标准

ISO/IEC 2700X 系列国际标准主要有以下几个方面：

ISO/IEC 27000　信息技术　安全技术　信息安全管理体系　概况与术语；

ISO/IEC 27001　信息技术　安全技术　信息安全管理体系　要求；

ISO/IEC 27002　信息技术　安全技术　信息安全管理实践规则；

ISO/IEC 27003　信息技术　安全技术　信息安全管理体系实施指南；

ISO/IEC 27004　信息技术　安全技术　信息安全管理　测量；

ISO/IEC 27005　信息技术　安全技术　信息安全风险管理；

ISO/IEC 27006　信息技术　安全技术　信息安全管理体系审核认证机构要求。

4.3.1 信息安全管理体系（ISO/IEC 27001：2005）

目前，在信息安全管理体系方面，ISO/IEC 27001：2005——信息安全管理体系标准已经成为世界上应用最广泛与最典型的信息安全管理标准，它是由英国标准 BS 7799 转换而成的。

本标准用于为建立、实施、运行、监视、评审、保持和改进信息安全管理体系（Information Security Management System，ISMS）提供模型。采用 ISMS 应当是一个组织的一项战略性决策。一个组织的 ISMS 的设计和实施受其需要和目标、安全要求、所采用的过程以及组织的规模和结构的影响，上述因素及其支持系统会不断发生变化。按照组织的需要实施 ISMS，是本标准所期望的，例如，简单的情况可采用简单的 ISMS 解决方案。

本标准可被内部和外部相关方用于一致性评估。

本标准采用一种过程方法来建立、实施、运行、监视、评审、保持和改进一个组织的 ISMS。

一个组织必须识别和管理众多活动使之有效运作。通过使用资源和管理，将输入转化为输出的任意活动，可以视为一个过程。通常，一个过程的输出可直接构成下一过程的输入。

一个组织内诸过程的系统的运用，连同这些过程的识别和相互作用及其管理，可称为“过程方法”。

本标准中提出的用于信息安全管理的过程方法鼓励其用户强调以下方面的重要性：

（1）理解组织的信息安全要求和建立信息安全方针与目标的需要；

（2）从组织整体业务风险的角度，实施和运行控制措施，以管理组织的信息安全风险；

（3）监视和评审 ISMS 的执行情况和有效性；

（4）基于客观测量的持续改进。

本标准采用了“规划（Plan）-实施（Do）-检查（Check）-处置（Act）”，简称 PDCA 模型，该模型可应用于所有的 ISMS 过程。图 4-2 说明了 ISMS 如何把相关方的信息安全要求和期望作为输入，并通过必要的行动和过程，产生满足这些要求和期望的信息安全结果。

采用 PDCA 模型还反映了治理信息系统和网络安全所设置的原则。本标准为风险评估、安全设计和实施、安全管理和再评估的原则提供了一个强健的模型。

例 1：某些信息安全缺陷不至于给组织造成严重的财务损失和/或使组织陷入困境，这可能是一种要求。

例 2：如果发生了严重的事件——可能是组织的电子商务网站被黑客入侵

——应有经充分培训的员工按照适当的程序，将事件的影响降至最小，这可能是一种期望。

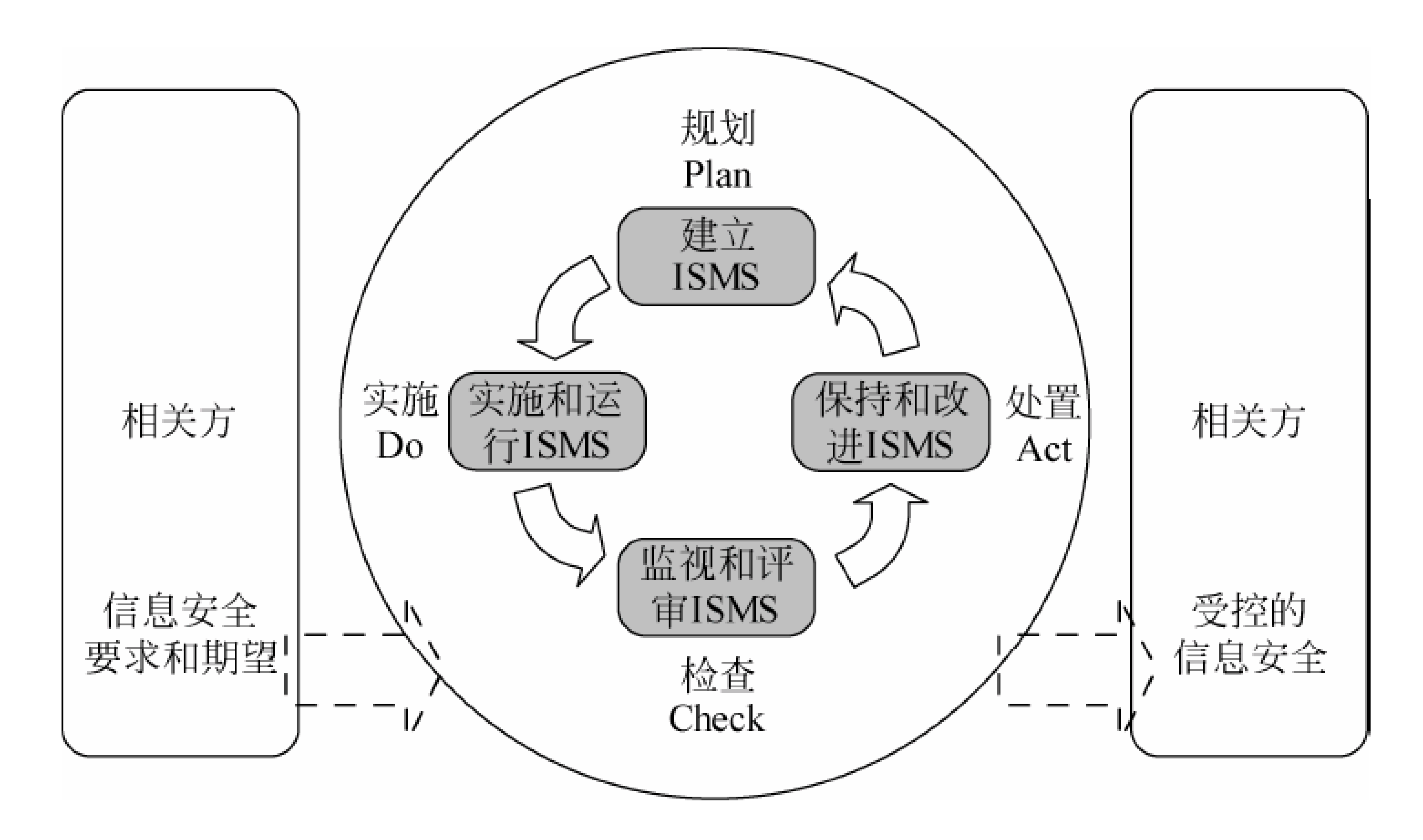


图 4-2　应用于 ISMS 过程的 PDCA 模型

表 4-1　PDCA 模型说明表

项　　目	说　　明
规划（建立 ISMS）	建立与管理风险和改进信息安全有关的 ISMS 方针、目标、过程和程序，以提供与组织总方针和总目标相一致的结果
实施（实施和运行 ISMS）	实施和运行 ISMS 方针、控制措施、过程和程序
检查（监视和评审 ISMS）	对照 ISMS 方针、目标和实践经验，评估并在适当时，测量过程的执行情况，并将结果报告管理者以供评审
处置（保持和改进 ISMS）	基于 ISMS 内部审核和管理评审的结果或者其他相关信息，采取纠正和预防措施，以持续改进 ISMS

与其他管理体系的兼容性。本标准与 GB/T 19001—2000 及 GB/T 24001—1996 相结合，以支持与相关管理标准一致的、整合的实施和运行。因此，一个设计恰当的管理体系可以满足所有这些标准的要求。

本标准的设计能够使一个组织将其 ISMS 与其他相关的管理体系要求结合或整合起来。

4.3.2　信息安全管理实施细则（ISO/IEC 27002）

国际标准化组织（ISO）发布公告，ISO/IEC 27002 将取代 ISO/IEC 17799：2005，直接由 ISO/IEC 17799：2005 更改标准编号为 ISO/IEC 27002：2005，于 2007 年 7 月实施。

ISO/IEC 27002 是一个被国际社会广泛认可的信息安全管理标准。其目的是将信息系统用于工业和商业用途时，为确定实施控制措施的范围提供一个参考依据，并且能够让各种规模的组织所采用。其前身 ISO/IEC 17799 于 2005 年进

行了修订，新版本增加了最新的信息处理技术应用、网络和通信技术，并更加强调了信息安全所涉及的商业问题和责任问题。它主要涵盖了 11 个控制域，其中包含 39 个控制目标以及 133 个控制措施。ISO/IEC 27002：2005 中的 11 个主题分别是：

（1）安全策略；

（2）信息安全组织；

（3）资产管理；

（4）人力资源管理安全；

（5）物理和环境安全；

（6）通信和操作管理；

（7）访问控制；

（8）信息系统获取、开发和维护；

（9）信息安全事件管理；

（10）业务连续性管理；

（11）符合性。

其结构如图 4-3 所示。

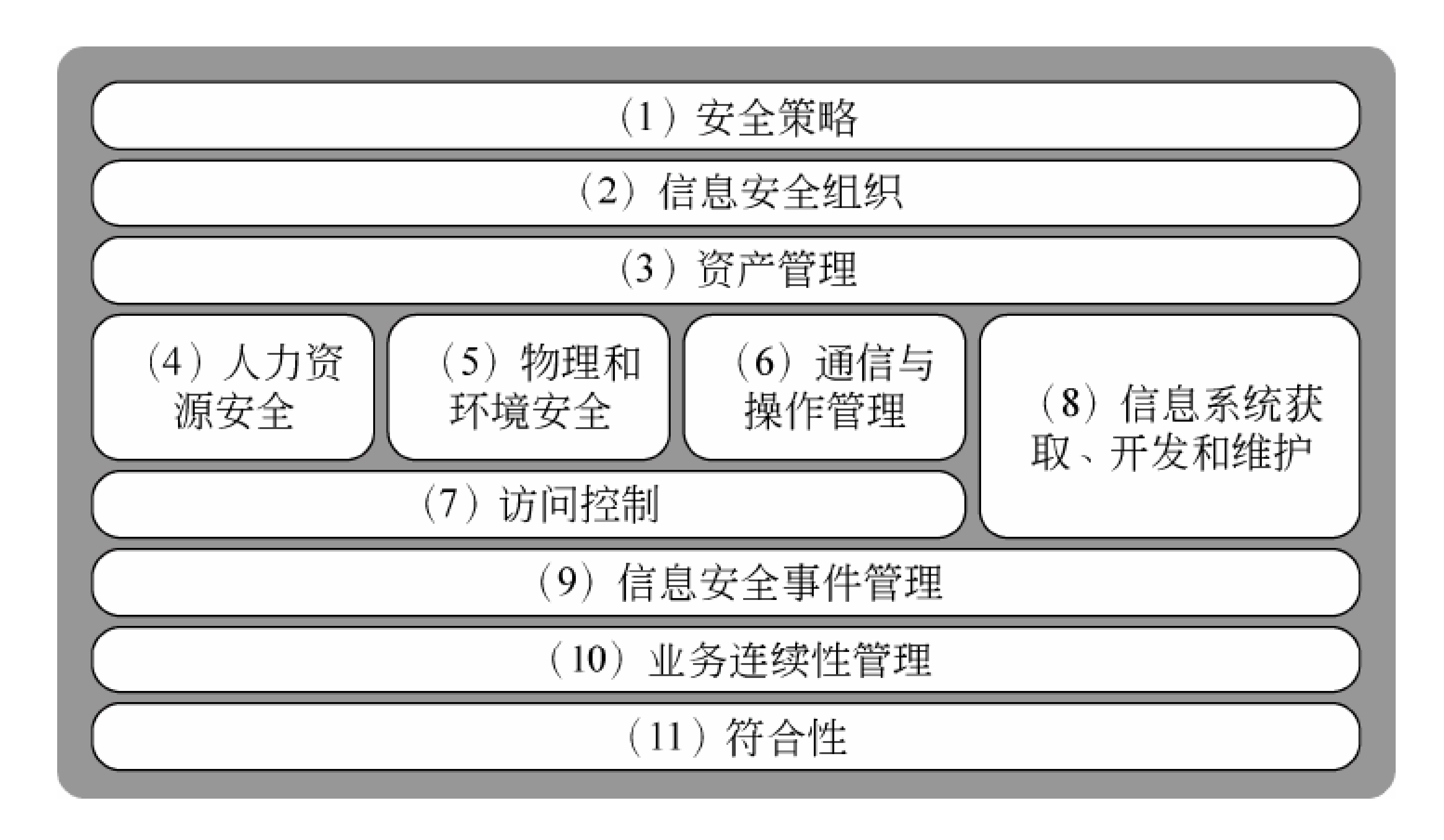


图 4-3　ISMS 架构图

ISO/IEC 27002 是一个完整的信息安全控制模型，它可以为企业带来以下好处：

（1）一个受业界广泛认同的方法论；

（2）按业界最佳实践方针去开展信息安全评估，实施、维护和管理；

（3）为定义策略、标准、流程和指南提供框架。

4.4　信息安全管理实施建议与指导类标准

信息安全管理实施建议与指导类标准主要有以下系列，其演进过程如图 4-4

所示。

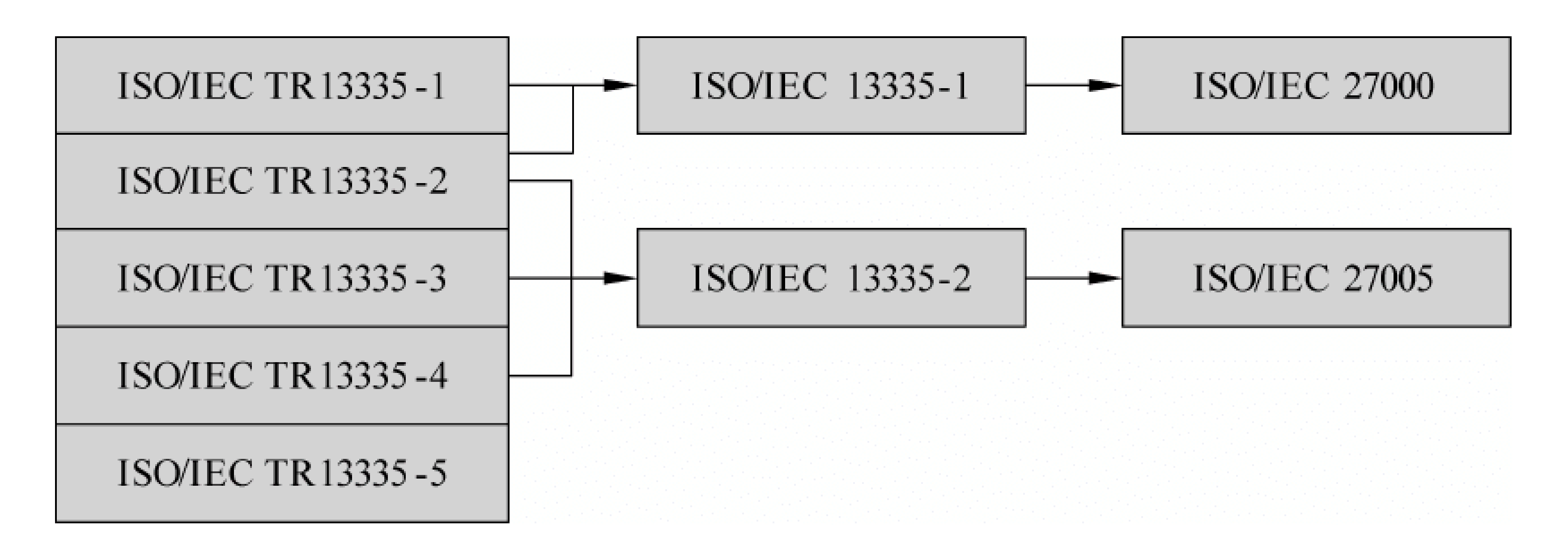


图 4-4　ISO/IEC TR 13335 的演进

（1）ISO/IEC TR 13335-1：1996　IT 安全的概念与模型；
（2）ISO/IEC TR 13335-2：1997　IT 安全管理与策划；
（3）ISO/IEC TR 13335-3：1998　IT 安全管理技术；
（4）ISO/IEC TR 13335-4：2000　防护措施的选择；
（5）ISO/IEC TR 13335-5：2001　网络安全管理指南。

ISO/IEC TR 13335，被称作“IT 安全管理指南”（Guidelines for the Management of IT Security，GMITS），新版称作“信息和通信技术安全管理”（Management of Information and Communications Technology Security，MICTS），是 ISO/IEC JTC1 制定的技术报告，是一个信息安全管理方面的指导性标准，其目的是要给出如何有效地实施 IT 安全管理的建议和指南。用户完全可以参照这个完整的标准制定出自己的安全管理计划和实施步骤。

该标准分为五个部分：

1．ISO/IEC TR 13335-1：1996《IT 安全的概念与模型》

IT 安全的概念和模型（Concepts and Models for IT Security），该部分包括了对 IT 安全和安全管理的一些基本概念和模型的介绍。

2．ISO/IEC TR 13335-2：1997《IT 安全管理与策划》

IT 安全的管理和计划（Managing and Planning IT Security），这个部分建议性地描述了 IT 安全管理和计划的方式、要点。

3．ISO/IEC TR 13335-3：1998《IT 安全管理技术》

IT 安全的技术管理（Techniques for the Management of IT Security），覆盖了风险管理技术、IT 安全计划的开发以及实施和测试，还包括一些后续的制度审查、事件分析、IT 安全教育程序等。

4．ISO/IEC TR 13335-4：2000《防护措施的选择》

防护的选择（Selection of Safeguards），它是最新发布的一个部分，主要探

讨如何针对一个组织的特定环境和安全需求来选择防护措施，这些措施不仅仅包括技术措施。

5．ISO/IEC TR 13335-5：2001《网络安全管理指南》

网络安全管理指南（Management Guidance on Network Security），这部分提供了关于网络和通信安全管理的指导性内容。该指南为识别和分析建立网络安全需求时需要考虑的相关通信因素提供支持，也包括对可能需要的安全措施的简要介绍。

4.5 信息安全测评标准

4.5.1 美国可信计算机安全评估标准（TCSEC）

TCSEC 标准是计算机系统安全评估的第一个正式标准，具有划时代的意义。该标准于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准，后来延至民用领域。TCSEC 将计算机系统的安全划分为四个等级、七个级别，如表 4-2 所示。

表 4-2 TCSEC 安全级别

类别	级别	名　称	主 要 特 征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取控制，高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

D 类安全等级：D 类安全等级只包括 D1 一个级别。D1 的安全等级最低。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

C 类安全等级：C 类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。C2 系统具有 C1 系统中所有的安全性特征。

B 类安全等级：B 类安全等级可分为 B1、B2 和 B3 三类。B 类安全系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。B2 系统必须满足 B1 系统的所有安全要求，而 B3 系统必须符合 B2 系统的所有安全需求。

A 类安全等级：A 系统的安全级别最高。目前，A 类安全等级只包含 A1

一个安全类别。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。

对于信息安全保障阶段，自欧洲四国（英国、法国、德国、荷兰）提出了评价满足保密性、完整性、可用性要求的信息技术安全评估标准（ITSEC）后，美国又联合以上诸国和加拿大，并会同国际标准化组织（ISO）共同提出信息技术安全评价的通用准则（CC for ITSEC），CC 已经被五个技术发达的国家承认为代替 TCSEC 的评价安全信息系统的标准，且将发展成为国际标准。

4.5.2　国际通用准则（CC）

CC 是国际标准化组织统一现有多种准则的结果，是目前最全面的评价准则。1996 年 6 月，CC 第一版发布；1998 年 5 月，CC 第二版发布；1999 年 10 月，CC v2. 1 版发布，并且成为 ISO 标准。CC 的主要思想和框架都取自 ITSEC 和 FC（信息技术安全评价联邦准则），并充分突出了“保护轮廓”的概念。CC 将评估过程划分为功能和保证两部分，评估等级分为 EAL1、EAL2、EAL3、EAL4、EAL5、EAL6 和 EAL7 共七个等级。每一级均需评估七个功能类，分别是配置管理、分发和操作、开发过程、指导文献、生命期的技术支持、测试和脆弱性评估。

CC 安全标准发展的过程如图 4-5 所示。第一个有关信息技术安全评估的标准诞生于 20 世纪 80 年代的美国，就是著名的“可信计算机系统评估标准”（TCSEC，又称橘皮书），该标准对计算机操作系统的安全性规定了不同的等级。从 20 世纪 90 年代开始，一些国家和国际组织相继提出了新的安全评估标准。1991 年，欧共体发布了“信息技术安全评估标准”（ITSEC）。1993 年，加拿大发布了“加拿大可信计算机产品评估标准”（CTCPEC），CTCPEC 综合了 TCSEC 和 ITSEC 两个标准的优点。同年，美国在对 TCSEC 进行修改补充并吸收 ITSEC 优点的基础上，发布了“信息技术安全评估联邦标准”（FC）。1993 年 6 月，上述国家共同起草了一份通用准则（CC），并将 CC 推广为国际标准。CC 发布的目的是建立一个各国都能接受的、通用的安全评估标准，国家与国家之间可以通过签订互认协议来决定相互接受的认可级别，这样能使基础性安全产品在通过 CC 准则评价并得到许可进入国际市场时，不需要再作评价。此外，国际标准化组织和国际电工委也已经制定了上百项安全标准，其中包括专门针对银行业务制定的信息安全标准。国际电信联盟和欧洲计算机制造商协会也推出了许多安全标准。

实际上，CC、ISO/IEC 15408、GB/T 18336 是同一个标准，只不过 CC 是最早的称谓，ISO/IEC 15408 是正式的 ISO 标准，GB/T 18336 则是我国等同采用 ISO/IEC 15408 之后的国标。

国际标准 ISO/IEC 15408 是为由联合技术委员会 ISO/IEC JTC1、信息技术与通用准则执行委员会、通用准则方案发起组织成员组成的一个实体合作而准

备的。ISO/IEC 15408 的同样的文章作为通用准则发表，被认定为信息技术安全性评估通用准则 2.0 版。通用准则附加信息和它的发起组织的联系信息由第 1 部分的附加部分提供。ISO/IEC 15408 的“信息技术安全性评估准则”由以下几部分组成：

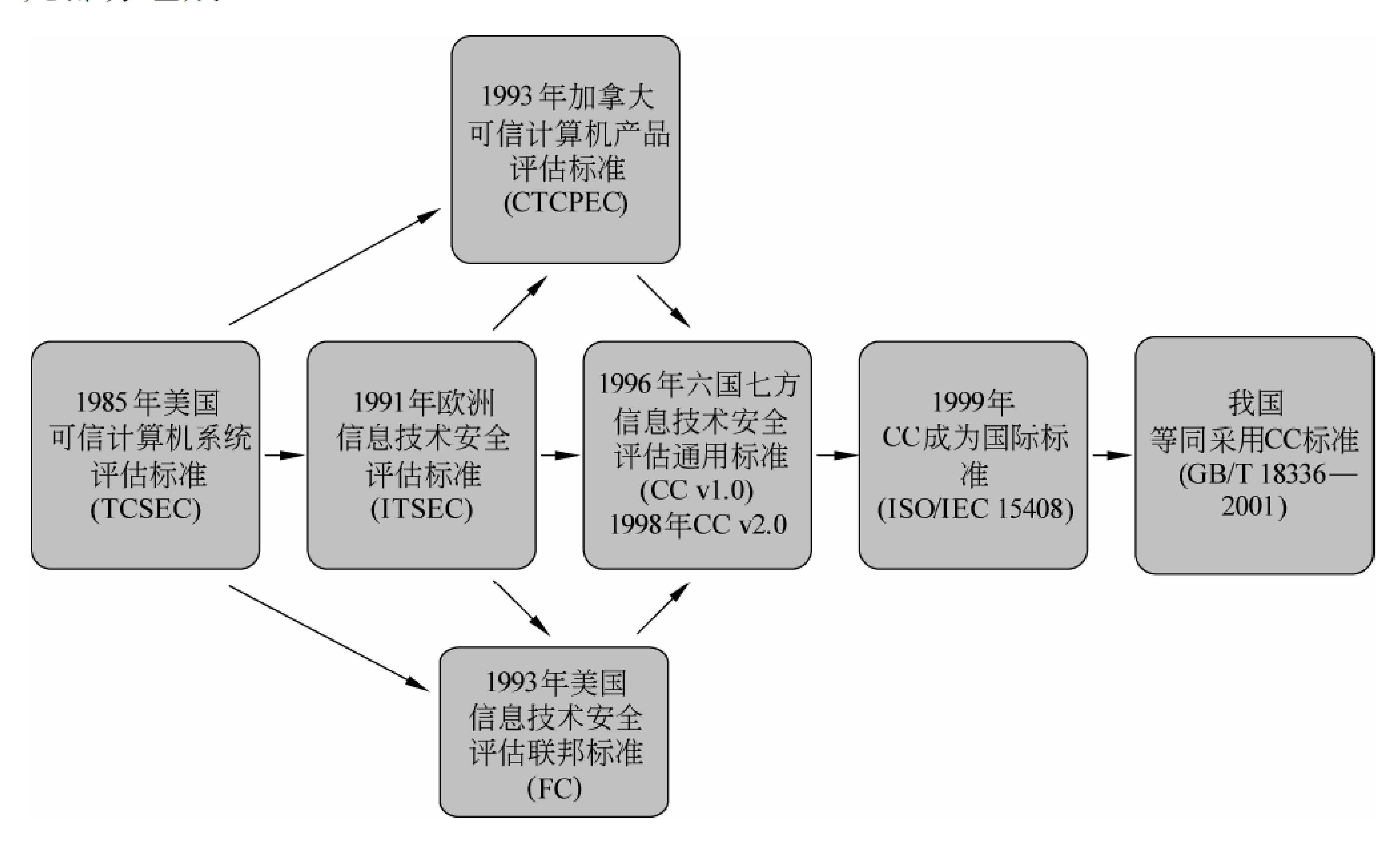


图 4-5 信息安全测评标准 CC 发展过程

（1）简洁和一般模型；
（2）安全功能要求；
（3）安全保证要求。

4.6 信息安全国家标准简介

1. GB/T 20945—2007《信息安全技术 信息系统安全审计产品技术要求和测试评价方法》

GB/T 20945—2007 规定了信息系统安全审计产品技术要求（安全功能要求、自身安全要求、性能要求和保证要求）和对应的测评方法。该标准将安全审计产品分为专用型和综合型两类。该标准对各类要求进行了详细规定，其中，安全功能要求包括审计踪迹、审计数据保护、安全管理、标识和鉴别、产品升级、监管要求；自身安全要求包括自身审计数生成、审计代理安全、管理信息传输和系统部署安全；性能要求包括稳定性、资源占用、网络影响、吞吐量；保证要求包括配置管理、交付与运行、测试脆弱性分析保证。标准以附录的形式给出了安全审计流程和跟踪涵盖的事件采集、事件处理和事件响应阶段。该

标准适用于信息系统审计产品的开发、测评和应用。该标准的目的是规范设计者如何设计和实现安全审计产品，并为安全审计产品的测试和应用提供技术支持和指导。

2．GB/T 20979—2007《信息安全技术　虹膜识别系统技术要求》

GB/T 20979—2007 规定了用虹膜识别技术为身份鉴别提供支持的虹膜识别系统的技术要求。

该标准详细规定了虹膜识别系统应具有的功能，包括自包含的、图像采集与处理、用户标识、用户识别、防伪造、警告与报警等功能；虹膜识别系统的基本要求包括错误接受率和拒绝率、响应时间、适用范围、使用安全条件；三个级别的基本功能、基本性能、自身安全功能、自身安全保证要求。标准以附录的形式介绍了虹膜识别的基本原理，给出了虹膜识别系统功能和性能要素与分等级要求的对应关系，以及主、客体的访问操作关系。

该标准适用于按信息安全等级保护要求所进行的虹膜识别系统的设计与实现，对虹膜识别系统的测试、管理也可参照使用。

3. GB/T 20983—2007《信息安全技术　网上银行系统信息安全保障评估准则》

GB/T 20983—2007 规定了网上银行系统的描述、安全环境、安全保证目的、安全保障要求，及网上银行系统信息安全保障目的和安全保障要求的符合性声明。

该标准对各类要求进行了详细规定，其中，系统描述包括网上银行系统描述、使命描述、系统概要和系统详细描述；安全环境包括假设、威胁、组织安全策略；安全保证目的包括安全保障的技术目标、管理目标和工程目标；特别详细规定了安全保障的各种要求，包括安全保障的技术要求、管理要求和工程要求。标准以附录的形式给出了网上银行系统信息安全保障符合性要求。

该标准适用于规范网上银行系统在网上交易过程中涉及信息安全的评估工作。

4．GB/T 20984—2007《信息安全技术　信息安全风险评估规范》

GB/T 20984—2007 规定了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。

该标准详细规定了风险评估框架及流程，包括风险的要素关系、分析原理、实施流程；风险评估实施，包括评估准备、资产识别、威胁识别、脆弱性识别、安全措施确认、风险分析；信息系统生命周期各阶段的风险评估，包括规划、设计、实施、运行维护、废弃各阶段的风险评估；风险评估的工作形式，包括自评估和检查评估。标准以附录的形式给出了风险的计算方法和风险评估的工具。

该标准适用于规范组织开展的风险评估工作。

5. GB/Z 20985—2007《信息技术　安全技术　信息安全事件管理指南》

GB/Z 20985—2007描述了信息安全事件的管理过程，提供了规划和制定信息安全事件管理策略和方案的指南，给出了管理信息安全事件和开展后续工作的相关过程和规程。

该标准详细规定了进行信息安全事件管理的背景，包括事件管理的目标和过程；信息安全事件管理方案的益处及需要应对的关键问题；规划和准备，包括信息安全的管理策略和管理方案、信息安全和风险管理策略、技术和其他支持、意识和培训；使用阶段，包括关键过程及信息安全事态和事件处理流程图、发现和报告、事态/事件评估和决策、响应；评审阶段，包括进一步的法律取证分析、经验教训、确定安全和方案的改进；改进阶段，包括安全风险分析和管理改进、改善安全状况、改进方案等。标准以附录的形式给出了信息安全事态和事件报告单示例、信息安全事件评估要点指南示例。

该标准可用于指导信息安全管理者，信息系统、服务和网络管理者对信息安全事件的管理。

该标准修改采用国际标准ISO/IEC TR 18044：2004《信息技术　安全技术　信息安全事件管理指南》。

6. GB/Z 20986—2007《信息安全技术　信息安全事件分类分级指南》

GB/Z 20986—2007为信息安全事件的分类分级提供指导，用于信息安全事件的防范与处置，为事前准备、事中应对、事后处理提供一个基础指南。

在该标准中，将信息安全事件分为七个基本类，即有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件、其他信息安全事件，每个基本类分别分为若干个子类，并对各个子类作了必要说明；根据信息系统的重要程度、系统的损失、社会的影响，将信息安全事件分为四个级，即特别重大事件、重大事件、较大事件、一般事件，并对每个级别列出了信息安全事件的若干情况。

该标准可供信息系统和基础信息传输网络的运营和使用单位以及信息安全主管部门参考使用。

7. GB/T 20987—2007《信息安全技术　网上证券交易系统信息安全保障评估准则》

GB/T 20987—2007规定了网上证券交易系统的描述、安全环境、安全保障目的、安全保障要求及网上证券系统信息安全保障目的和安全保障要求的符合性声明。

该标准首先对网上证券交易系统进行了详细描述，并给出了信息系统的框架和参考模型。然后详细规定了安全环境，包括假设、威胁、组织安全策略；

安全保障目的，包括安全保障的技术目标、管理目标、工程目标；安全保障要求，包括安全保障的技术要求、管理要求、工程要求。标准以附录的形式给出了网上证券系统信息安全保障的符合性声明，包括安全保障的目的和要求的符合性声明，并给出了安全保障的技术目标与技术要求、管理目标与管理要求、工程目标与工程要求的映射关系。

该标准适用于规范网上证券系统在交易过程中涉及信息安全的评估工作。

8. GB/T 20988—2007《信息安全技术　信息系统灾难恢复规范》

GB/T 20988—2007 规定了信息系统灾难恢复应遵守的基本要求。

该标准详细规定了灾难恢复一般事项，包括灾难恢复的工作范围、组织机构、规划的管理、外部协作、审计和备案；灾难恢复需求的确定，包括风险分析、业务影响分析、确定灾难恢复目标；灾难恢复的制定，包括灾难恢复策略制定的要素、资源的获取方式、资源的要求；灾难恢复策略的实现，包括灾难备份系统技术方案的实现、灾难备份中心的选择和建设、运行维护管理能力和灾难恢复预案的实现。标准以附录的形式给出了灾难恢复能力的等级划分、灾难恢复预案框架。

该标准适用于信息系统灾难恢复的规划、审批、实施和管理。

9. GB/T 21028—2007《信息安全技术　服务器安全技术要求》

GB/T 21028—2007 依据 GB 17859—1999《计算机信息系统　安全保护等级划分准则》划分的五个安全保护等级，规定了服务器所需要的安全技术要求，以及每一个安全保护等级的不同安全技术要求。

该标准详细规定了服务器的安全功能要求和安全分等级要求。其中，服务器安全功能要求包括设备安全、运行安全和数据安全；服务器安全分等级要求包括五个安全保护等级各自涵盖的安全功能要求和安全保证（含服务器安全子系统的自身安全保护、设计和实现、管理）要求。标准还以附录的形式给出了服务器安全方面有关概念的说明。

该标准适用于按 GB 17859—1999 的五个安全保护等级要求所进行的等级化服务器的设计、实现、选购和使用。按五个等级对服务器安全进行的测试和管理也可参照使用。

10. GB/T 21050—2007《信息安全技术　网络交换机安全技术要求（评估保证级 3）》

GB/T 21050—2007 依据 GB/T 18336—2001《信息技术　安全技术　信息技术安全性评估准则》的要求，规定了网络交换机评估保证级（EAL）的 EAL3 级的安全技术要求，主要包括安全环境，以及网络交换机 EAL3 级的安全目的、安全功能要求和安全保证要求。

该标准首先介绍了什么是网络交换机。然后详细规定了网络交换机的安全

环境，包括安全假设、威胁和组织策略等；安全目的，包括网络交换机 EAL3 级的安全目的、环境安全目的；安全要求，包括安全功能要求和安全保证要求。标准以附录的形式给出了安全环境与安全目的、安全要求与安全目的之间的关系及其合理性说明，还给出了安全功能要求的应用注释。

该标准适用于网络交换机的研制、开发、测试、评估和采购，使用对象主要是信息系统安全工程师、产品生产商、安全产品评估者。

11. GB/T 21052—2007《信息安全技术 信息系统物理安全技术要求》

GB/T 21052—2007 依据 GB 17859—1999《计算机信息系统 安全保护等级划分准则》划分的五个安全保护等级，规定了信息系统物理安全的各种技术要求。

该标准详细规定了信息系统第一、二、三、四级的物理安全技术要求，包括上述各级的设备物理安全技术要求、环境物理安全技术要求、系统物理安全技术要求，以及各级别设备安全技术要求的具体项目。标准还以附录的形式给出了信息系统物理安全方面有关概念的说明。

该标准适用于按 GB 17859—1999 的五个安全保护等级要求所进行的等级化的信息系统物理安全的设计和实现，对按 GB 17859—1999 的安全保护等级的要求对信息系统物理安全测试、管理也可参照使用。

12. GB/T 21053—2007《信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求》

GB/T 21053—2007 参照 GB 17859—1999《计算机信息系统 安全保护等级划分准则》划分的五个安全保护等级，对 PKI 系统安全保护进行等级划分，规定了不同等级 PKI 系统所需要满足的评估内容。

该标准详细规定了 PKI 系统第一、二、三、四、五级的安全保护技术要求，包括上述各级的物理安全、角色与责任、访问控制、标识与鉴别、数据输入输出、密钥管理、轮廓管理、证书管理、配置管理、分发和操作、开发、指导性文档、生命周期支持、测试，以及审计、备份与恢复、脆弱性评定。标准以附录的形式给出了 PKI 系统安全要素各个要求级别的划分。

该标准适用于 PKI 的安全保护等级的评估，对于 PKI 系统安全功能的研制、开发、测试和产品采购亦可参照使用。

13. GB/T 21054—2007《信息安全技术 公钥基础设施 PKI 系统安全等级保护评估准则》

GB/T 21054—2007 依据 GB 17859—1999《计算机信息系统 安全保护等级划分准则》划分的五个安全保护等级，规定了不同等级 PKI 系统所需要的安全技术要求。

该标准详细规定了 PKI 系统第一、二、三、四、五级的安全评阅内容，包

括上述各级的物理安全、角色与责任、访问控制、标识与鉴别、数据输入输出、密钥管理、轮廓管理、证书管理，以及审计、备份与恢复。标准以附录的形式给出了 PKI 系统安全要素各个要求级别的划分。

该标准适用于 PKI 系统的设计和实现，对于 PKI 系统安全功能的研制、开发、测试和产品采购亦可参照使用。

4.7　国家信息安全等级保护体系

信息安全等级保护制度是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。实行信息安全等级保护制度，能够充分调动国家、法人和其他组织及公民的积极性，发挥各方面的作用，达到有效保护的目的，增强安全保护的整体性、针对性和实效性，使信息系统安全建设更加突出重点、统一规范、科学合理，对促进我国信息安全的发展将起到重要推动作用。

为了进一步提高信息安全保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定：“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。”2003 年中央办公厅、国务院办公厅转发的《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）明确指出：“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南。”

4.7.1　国家信息安全保障工作的主要内容

国家信息安全保障工作的主要内容如下：

（1）信息安全等级保护制度；

（2）信息保护和网络信任体系建设；

（3）信息安全监控体系；

（4）信息安全应急处理；

（5）信息安全技术研究，信息安全产业发展；

（6）信息安全法制建设和标准化建设；

（7）信息安全人才培养；

（8）保证信息安全资金；

（9）信息安全工作的领导，信息安全责任制。

1. 什么是信息安全等级保护

信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

根据信息和信息系统在国家安全、经济建设、社会生活中的重要程度，根据信息和信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度，针对信息的保密性、完整性和可用性要求及信息系统必须要达到的基本的安全保护水平等因素，信息和信息系统的安全保护等级共分五级：

（1）自主保护级：适用于一般的信息和信息系统，其受到破坏后，会对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益。

（2）指导保护级：适用于一定程度上涉及国家安全、社会秩序、经济建设和公共利益的一般信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成一定损害。

（3）监督保护级：适用于涉及国家安全、社会秩序、经济建设和公共利益的信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成较大损害。

（4）强制保护级：适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成严重损害。

（5）专控保护级：适用于涉及国家安全、社会秩序、经济建设和公共利益的重要信息和信息系统的核心子系统，其受到破坏后，会对国家安全、社会秩序、经济建设和公共利益造成特别严重损害。

实施信息安全等级保护的主要依据：

（1）《中华人民共和国计算机信息系统安全保护条例 》（国务院 147 号令）：“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定。”

（2）《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）：“要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统，抓紧建立信息安全等级保护制度，制定信息安全等级保护的管理办法和技术指南。”

（3）《国家信息安全战略》：“继续完善和实施信息安全等级保护制度，科学确定安全保护等级，开展相应等级的安全建设和管理。”

（4）《国民经济和社会发展第十二个五年规划纲要》：“实施信息安全等级保护制度，加强信息网络监测、管控能力建设，确保基础信息网络和重点信息系

统安全。”

（5）《国务院关于推进信息化发展和切实保障信息安全的若干意见》：“落实信息安全等级保护制度，开展相应等级的安全建设和管理，做好信息系统定级备案、整改和监督检查。”

职责分工：

公安机关牵头，制定政策标准，并进行监督、检查、指导。国家保密部门、密码管理部门负责有关保密工作和密码工作的监督、检查、指导。工信部及地方经信部门负责等级保护工作中部门间的协调，其中涉及国家秘密信息系统由国家保密部门负责，非涉及国家秘密信息系统由公安机关负责

2．信息安全等级保护工作的主要内容

（1）定级：将信息系统（包括网络）按照重要性和遭受损坏后的危害性分成五个安全保护等级。

（2）备案：等级确定后，第二级（含）以上信息系统到公安机关备案，公安机关审核后颁发备案证明。

（3）测评：备案单位选择符合国家规定条件的测评机构开展等级测评。

（4）建设整改：备案单位根据信息系统安全等级，按照国家政策、标准开展安全建设整改。

（5）检查：公安机关定期开展监督、检查、指导。

4.7.2　开展等级保护工作依据的政策和标准

1．信息安全等级保护政策体系

近几年，公安部根据国务院 147 号令的授权，会同国家保密局、国家密码管理局、发改委、原国务院信息办出台了一些文件，公安部对有些具体工作出台了一些指导意见和规范，构成了信息安全等级保护政策体系。

图 4-6 所示为等级保护工作配套政策体系的框图。

（1）《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）；

（2）《信息安全等级保护管理办法》（公通字[2007]43 号）；

（3）《关于开展全国重要信息系统安全等级保护定级工作的通知》（公通字[2007]861 号）；

（4）《信息安全等级保护备案实施细则》（公信安[2007]1360 号）；

（5）《关于开展信息系统等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）；

（6）《关于做好信息安全等级保护测评机构审核推荐工作的通知》（公信安[2010]559 号）；

（7）《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》（发改高技[2008]2071 号）；

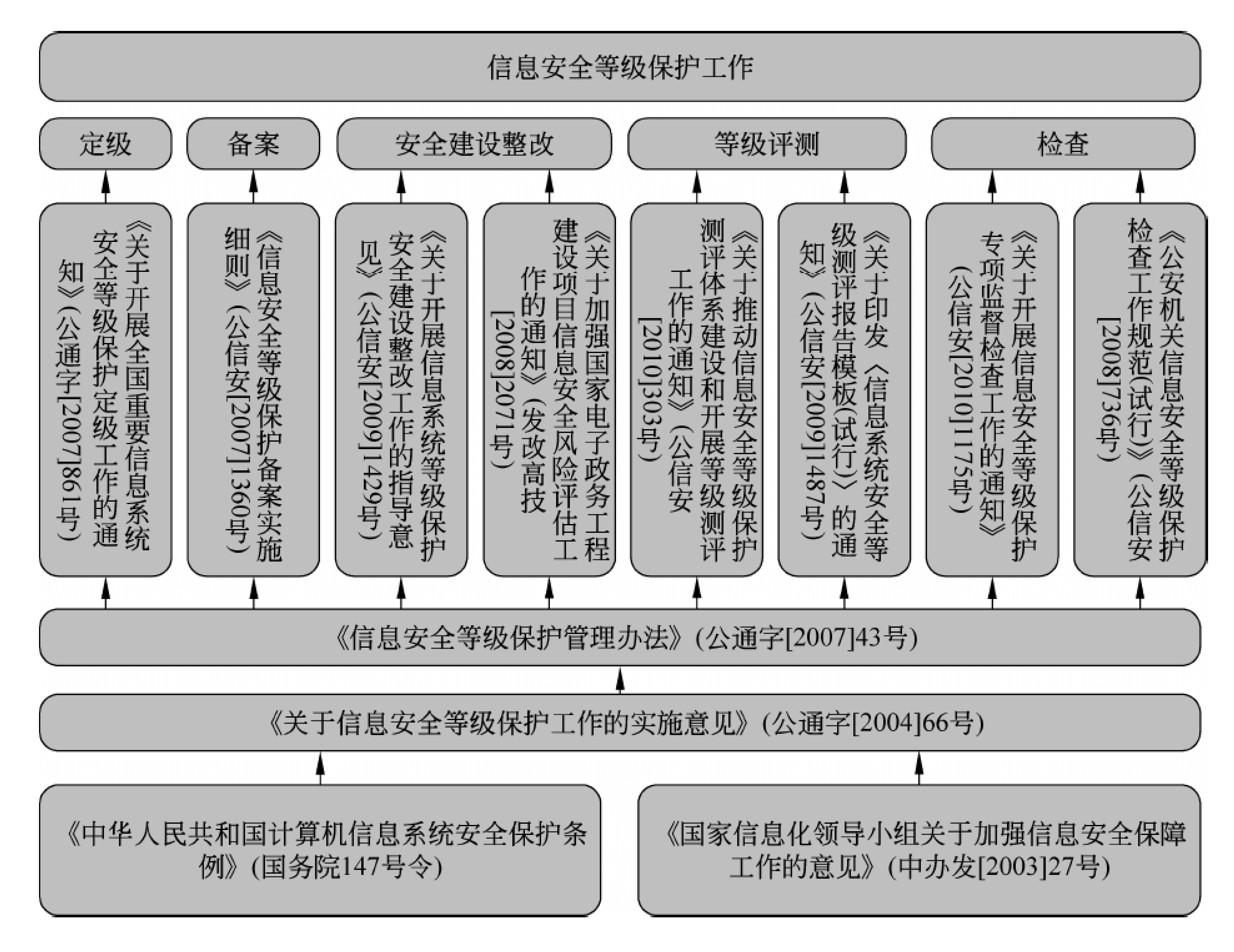


图 4-6 等级保护工作配套政策体系的框图

（8）《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号）；

（9）《关于印发〈信息系统安全等级测评报告模板（试行）〉的通知》（公信安[2009]1487 号）；

（10）《公安机关信息安全等级保护检查工作规范》（公信安[2008]736 号）；

（11）《关于开展信息安全等级保护专项监督检查工作的通知》（公信安[2010]1175 号）；

（12）《关于进一步推进中央企业信息安全等级保护工作的通知》（公通字[2010]70 号）。

2．信息安全等级保护标准体系

多年来，在有关部门支持下，在国内有关专家、企业的共同努力下，全国信息安全标准化技术委员会和公安部信息系统安全标准化技术委员会组织制定了信息安全等级保护工作需要的一系列标准，形成了比较完整的信息安全等级保护标准体系。汇集成《信息安全等级保护标准汇编》供有关单位、部门使用，如图 4-7 所示。

（1）基础标准：GB 17859—1999《计算机信息系统　安全保护等级划分准则》，在此基础上制定出技术类、管理类、产品类标准。

（2）安全要求：GB/T 22239—2008《信息安全技术　信息系统安全等级保护基本要求》——信息系统安全等级保护的行业规范。

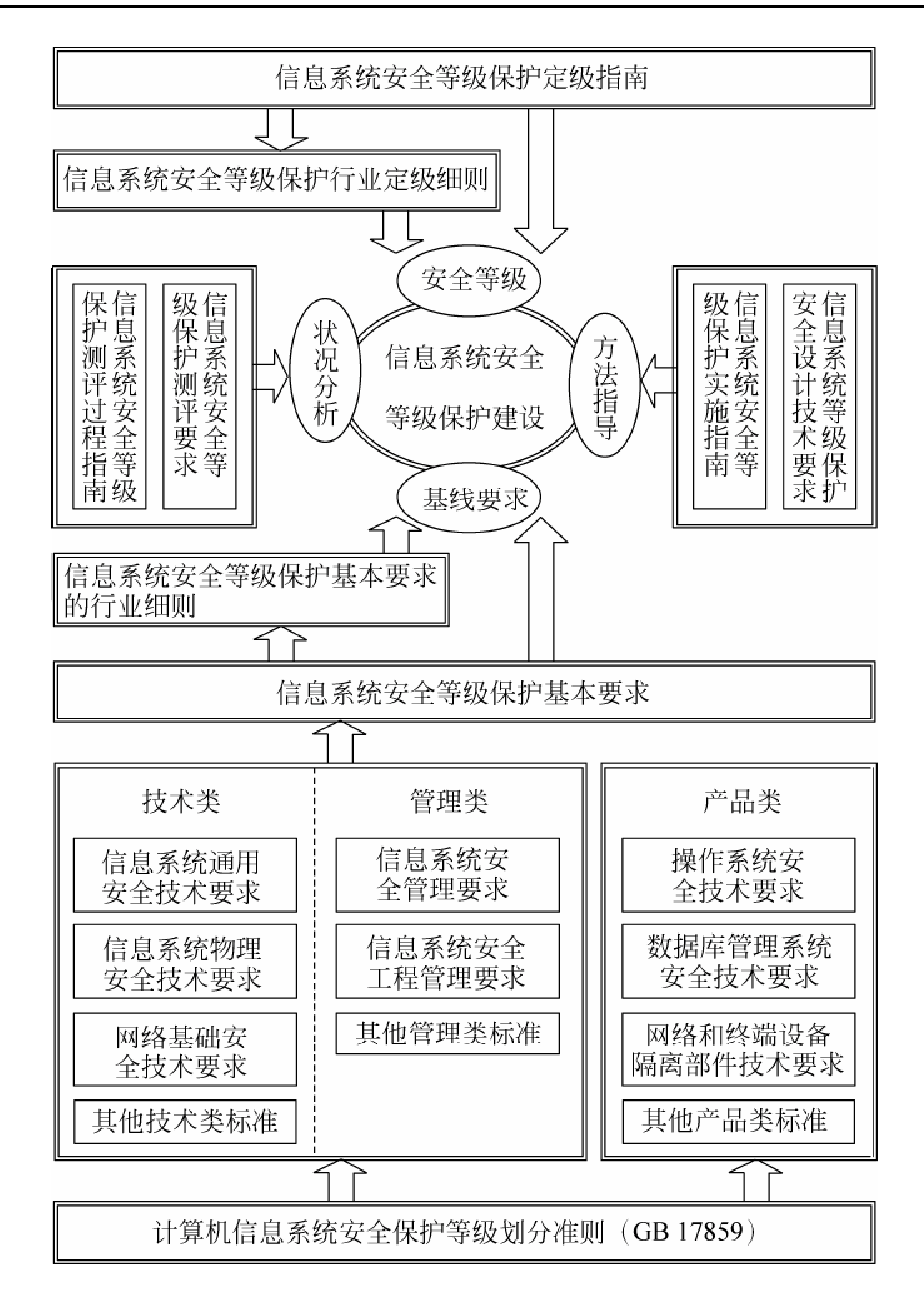


图 4-7　信息安全等级保护标准体系

（3）系统等级：GB/T 22240—2008《信息安全技术　信息系统安全等级保护定级指南》——信息系统安全等级保护行业定级细则。

（4）方法指导：《信息系统安全等级保护实施指南》、《信息系统等级保护安全设计技术要求》。

（5）现状分析：《信息系统安全等级保护测评要求》、《信息系统安全等级保护测评过程指南》。

4.7.3　等级保护工作的具体内容和要求

1．信息安全等级保护定级工作

1）信息系统定级原则

自主定级、专家评审、主管部门审批、公安机关审核。具体可按照《关于

开展全国重要信息系统安全等级保护定级工作的通知》(公通字[2007]861 号)要求执行。

2）定级工作流程

摸底调查、确定定级对象、对信息系统进行重要性分析、确定信息系统安全保护等级、组织专家评审、主管部门审批、公安机关审核。

（1）摸底调查。要开展对本行业、本部门所有信息系统的摸底调查，摸清信息系统底数，全面掌握信息系统（包括信息网络）的数量、分布、业务类型、应用或服务范围、系统结构等基本情况。

（2）确定定级对象。起支撑、传输作用的信息网络（包括专网、内网、外网、网管系统）；用于生产、调度、管理、指挥、作业、控制、办公等目的的各类业务系统；各单位网站。

（3）确定信息系统安全保护等级。根据信息系统重要性分析结论，按照《信息安全等级保护管理办法》要求确定等级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

实际操作中参考确定信息系统等级：

第一级信息系统：适用于小型私营、个体企业、中小学、乡镇所属信息系统及县级单位中一般的信息系统。

第二级信息系统：适用于县级某些单位中的重要信息系统；地市级以上国家机关、企事业单位内部一般的信息系统。例如，非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。

2. 信息系统备案工作

备案工作包括信息系统备案、受理、审核和备案信息管理。具体按照《关于开展全国重要信息系统安全等级保护定级工作的通知》要求开展。

1）备案

第二级以上信息系统，由中央企业到所在地市级以上公安机关网络安全保卫部门办理备案手续，填写《信息系统安全等级保护备案表》。

在京央企，其跨省或者全国统一联网运行并由总部统一定级的信息系统，由总公司向公安部备案；其他信息系统向北京市公安局备案。

非在京央企，其信息系统向当地市级以上公安机关备案。

跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，应

当向当地公安机关备案。

2）受理备案与审核

公安机关受理备案，按照《信息安全等级保护备案实施细则》要求，对备案材料进行审核，定级准确、材料符合要求的颁发由公安部统一监制的备案证明。发现定级不准的，通知备案单位重新审核确定。

3）备案管理

将备案信息系统录入重要信息系统安全管理系统进行管理。

3．信息安全等级保护测评工作

等级测评是测评机构依据国家信息安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密信息系统安全等级保护状况进行检测评估的活动，是信息安全等级保护工作的重要环节。

公安机关按照《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号）要求，开展测评机构和测评人员的管理工作，保证等级测评的客观、公正和安全。

1）测评目的

一是掌握信息系统安全状况、排查系统安全隐患和薄弱环节、明确信息系统安全建设整改需求；二是能够衡量出信息系统安全保护措施是否符合等级保护基本要求，是否具备了相应等级的安全保护能力。

2）等级测评工作的开展

聘请《全国信息安全等级保护测评机构推荐目录》中的测评机构，对已定级备案的信息系统开展等级测评，查找与相关标准要求之间的差距，分析系统在安全管理、安全技术措施等方面存在的安全问题，确定信息系统安全建设整改需求，为开展信息系统安全建设整改提供依据。

（1）测评时机：① 建设整改前开展等级测评，现状分析；② 建设整改后开展等级测评，检验整改效果。

（2）测评频率：第三级以上定期；第二级参照。

（3）测评费用：参照国家信息化项目人工计费标准或根据被测设备数量与测评项预算测评费用。

3）测评机构和测评人员的管理

国家信息安全等级保护工作协调小组办公室（以下简称“等保办”）发布《全国信息安全等级保护测评机构推荐目录》。公安部信息安全等级保护评估中心（以下简称“评估中心”）负责测评机构的能力评估和培训工作。

4．信息系统安全建设整改工作

1）工作目标

实现五方面目标：一是信息系统安全管理水平明显提高，二是信息系统安全防范能力明显增强，三是信息系统安全隐患和安全事故明显减少，四是有效保障信息化健康发展，五是有效维护国家安全、社会秩序和公共利益。

2）工作范围和工作特点

工作范围：已备案的第二级（含）以上信息系统纳入安全建设整改的范围。尚未开展定级备案的信息系统，要先定级备案，定级不准的要先纠正，再开展安全建设整改。新建系统要同步开展安全建设工作。

工作特点：继承发展、引入标准、外部监督、政策牵引。

3）工作方法

突出重要系统，兼顾二级。试点示范，行业推广。管理制度建设和技术措施建设并重。加固改造，缺什么补什么；也可以进行总体安全建设整改规划。利用信息安全等级保护综合工作平台，使等级保护工作常态化。

4）工作内容

以《信息系统安全等级保护基本要求》为目标，从管理和技术两方面进行安全建设整改。

（1）等级保护安全管理建设整改：一是落实信息安全责任制，二是落实人员安全管理制度，三是落实系统建设管理制度，四是落实系统运维管理制度。

（2）等级保护安全技术措施建设整改：结合行业特点和安全需求，制定符合相应等级要求的信息系统安全技术建设整改方案，开展安全技术措施建设，落实相应的物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施。

可以采取“一个中心三维防护（即一个安全管理中心和计算环境安全、区域边界安全和通信网络安全）”策略，实现相应级别信息系统的安全保护技术要求，如图 4-8 所示。

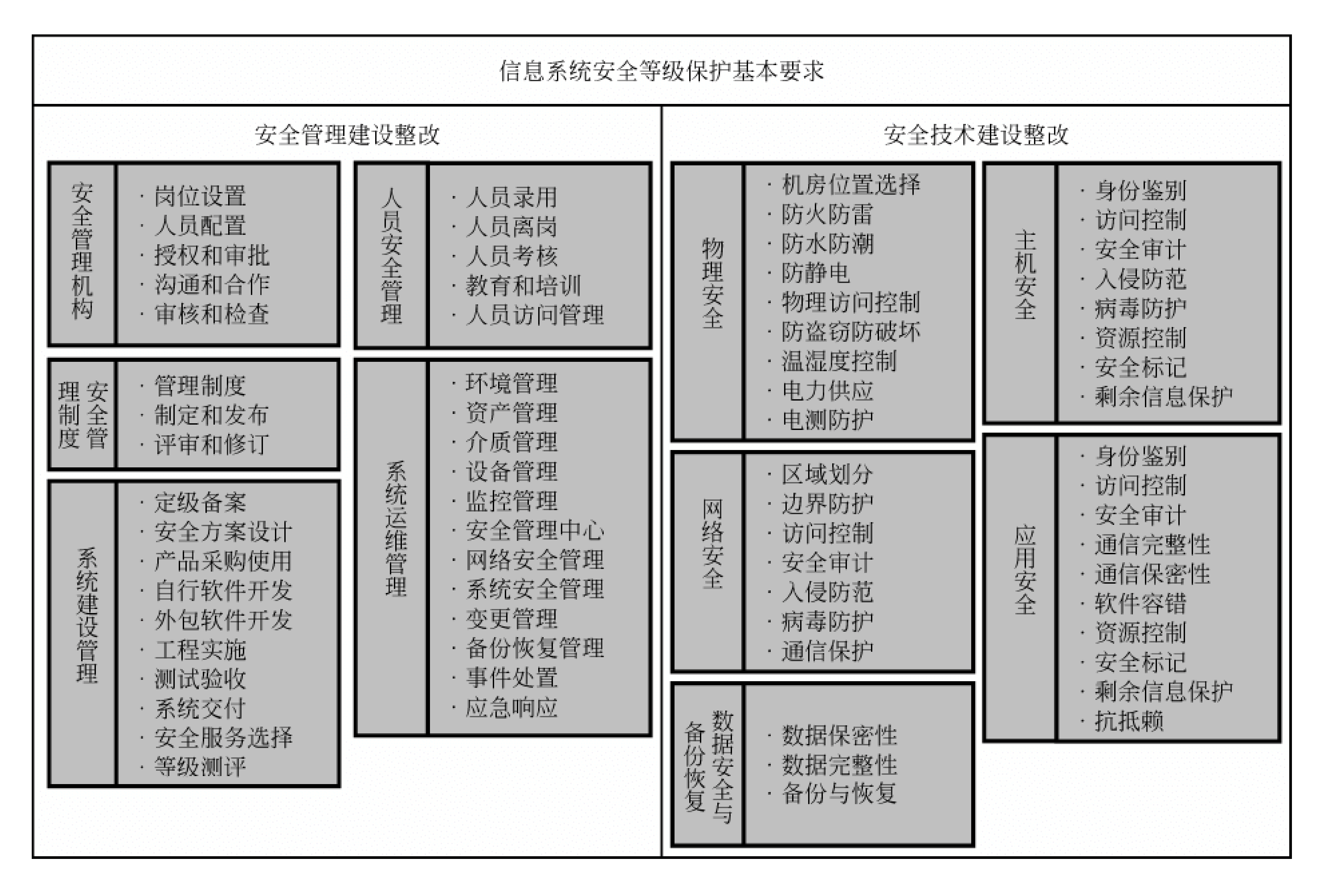


图 4-8 信息安全等级保护基本要求

5）工作流程

开展信息安全等级保护的工作流程如图 4-9 所示。第一步，制定安全建设整改工作规划，对安全建设整改工作进行总体部署；第二步，开展等级测评，对信息系统进行安全现状分析，从管理和技术两方面确定安全建设整改需求；第三步，确定安全保护策略，制定信息系统安全建设整改方案；第四步，开展信息系统安全建设整改工作，建立并落实安全管理制度，落实安全责任制，建设安全设施，落实安全措施；第五步，开展安全自查和等级测评，及时发现问题并进一步整改。

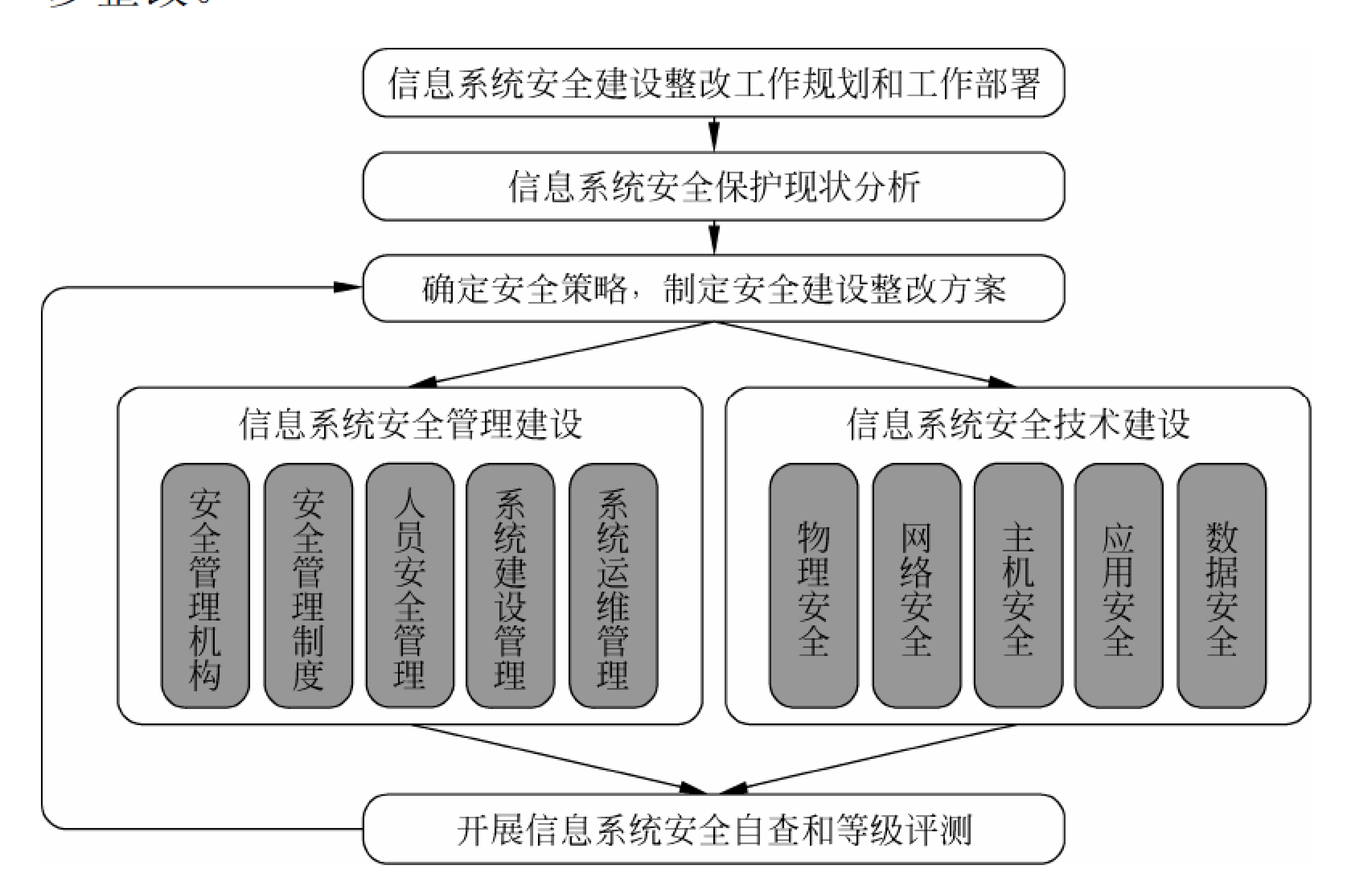


图 4-9　开展信息安全等级保护的工作流程

6）信息系统应达到的保护能力目标

第二级信息系统：经过安全建设整改工作，信息系统具有抵御小规模、较弱强度恶意攻击的能力，抵抗一般的自然灾害的能力，防范一般性计算机病毒和恶意代码危害的能力；具有检测常见的攻击行为，并对安全事件进行记录的能力；系统遭到损害后，具有恢复系统正常运行状态的能力。

第三级信息系统：经过安全建设整改工作，信息系统在统一的安全保护策略下具有抵御大规模、较强恶意攻击的能力，抵抗较为严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保障性要求高的系统，应能立即恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

第四级信息系统：经过安全建设整改工作，信息系统在统一的安全保护策略下具有抵御敌对势力有组织的大规模攻击的能力，抵抗严重的自然灾害的能力，防范计算机病毒和恶意代码危害的能力；具有检测、发现、报警、记录入侵行为的能力；具有对安全事件进行快速响应处置，并能够追踪安全责任的能力；在系统遭到损害后，具有能够较快恢复正常运行状态的能力；对于服务保

障性要求高的系统，应能迅速恢复正常运行状态；具有对系统资源、用户、安全机制等进行集中控管的能力。

5. 安全自查和监督检查

1）备案单位的定期自查

定期开展自查，掌握信息系统安全状况、安全管理制度及技术保护措施的落实情况等。配合公安机关的监督检查工作，如实提供有关资料及文件。当重要信息系统发生事件、案件时，备案单位应当及时向受理备案的公安机关报告。

2）行业主管部门的督导检查

行业主管部门要建立督导检查制度，组织制定本行业、本部门的信息安全等级保护检查工作规范。定期组织对本行业、本部门等级保护工作开展情况进行检查，督促落实信息安全等级保护制度，达到重点督促，以点带面的目的。

3）公安机关的监督检查

依据《关于开展信息安全等级保护专项监督检查工作的通知》（公信安[2010]1175）和《公安机关信息安全等级保护检查工作规范（试行）》开展监督检查，会同主管部门共同开展、建立监督检查配合机制。对重要信息系统发生的事件、案件及时进行调查和立案侦查，并指导开展应急处置工作。

具体检查内容主要有：等级保护工作部署和组织实施情况；信息系统安全等级保护定级备案情况；信息安全设施建设和信息安全整改情况；信息安全管理制度建立和落实情况；信息安全产品选择和使用情况；聘请测评机构开展技术测评工作情况；定期自查情况。

4.7.4 中央企业开展等级保护工作要求

（1）出台行业等级保护政策、标准，为全面贯彻落实等级保护制度提供政策和技术保障。目前40余个重要行业出台了100余份行业等级保护政策文件，20余个重要行业出台了40余份行业等级保护标准。

（2）组织全行业开展信息系统定级备案工作，摸清本行业重要信息网络、信息系统基本情况，汇编行业重要信息系统名录。

（3）组织开展信息系统等级测评，及时掌握重要信息系统安全保护状况，出台年度重要信息系统安全状况分析报告，为领导和综合部门决策提供支持。

（4）组织开展信息安全等级保护安全建设整改工作，着力提高信息系统整体保护能力。

（5）进一步开展多层次全方位的信息安全教育培训，提高安全意识和工作能力。

（6）加强实时监测和分析研判，提高网络安全的发现预警能力。

（7）制定应急处置预案，加强应急演练，提高网络应急处置能力。

（8）加强灾备建设，提高网络快速恢复能力。

（9）建立多方协调配合机制，有效发挥各方力量。

（10）加大人员和资金投入，提高安全保障能力。

第5章 云计算安全

从云计算概念的提出发展至今，云计算经历了定义逐渐清晰、应用逐渐增多、产业逐渐形成的各个阶段。云计算提供了开放的标准、可伸缩的系统和面向服务架构，使组织能够以灵活且经济实惠的方式提供可靠的、随需应变的服务。云计算在提供方便易用与低成本特性的同时也带来了新的挑战，安全问题首当其冲，它成为了制约云计算发展的关键因素之一，能否确保云计算平台的机密性、完整性、可用性，将很大程度影响用户是否愿意将其数据和应用向云计算平台进行迁移。本章旨在探讨云计算技术和系统的安全问题，并针对云计算系统的多种服务模式，“软件即服务”、“数据即服务”、“平台即服务”、“网络即服务”、“架构即服务”，提出了一个面向云计算系统的安全架构，论述了国内外的云计算安全标准发展现状，最后进一步分析了主要云计算提供商的安全解决方案。

5.1 云计算安全问题分析

根据咨询公司 IDC 的市场调查，业界对云计算大规模商用尚存在一些疑虑，主要表现在对云计算系统的安全性、效率、与现有 IT 系统的兼容性、可定制化、资费、法规和标准的缺失等方面，其中安全性是有待解决的最主要的问题之一，如图 5-1 所示。

5.1.1 云计算的主要安全威胁分析

咨询公司 Gartner 总结了七个主要的云安全威胁：优先访问权风险、管理权限风险、数据处所风险、数据隔离风险、数据恢复风险、调查支持风险、长期发展风险。概括地说，当企业将他们的敏感数据和文档迁移到云计算系统中后，数据和信息管理流程将对这些企业不再透明，他们将不再知道自己的数据存储在哪里、被怎么存储的、谁在处理、有没有备份等信息。这个现象同时也是云计算系统中的诸多安全挑战的最主要根源。就好比历史上当银行出现以后，人们也是在建立了对银行系统足够的信任以后才开始将货币存到银行中的。类似

的，建立云计算供应商和用户之间的互信同样需要相当长的一段时间。它需要云计算产业链各个环节的企业和组织的共同努力，当然，有效地解决上述问题和挑战也是必不可少的。在接下来的章节中，我们首先对有代表性的云计算系统安全分析文献进行了回顾，而后讨论了如何从多种云计算服务模式的角度设计云计算安全架构，最后讨论了几个有待解决的问题和今后的研究方向。

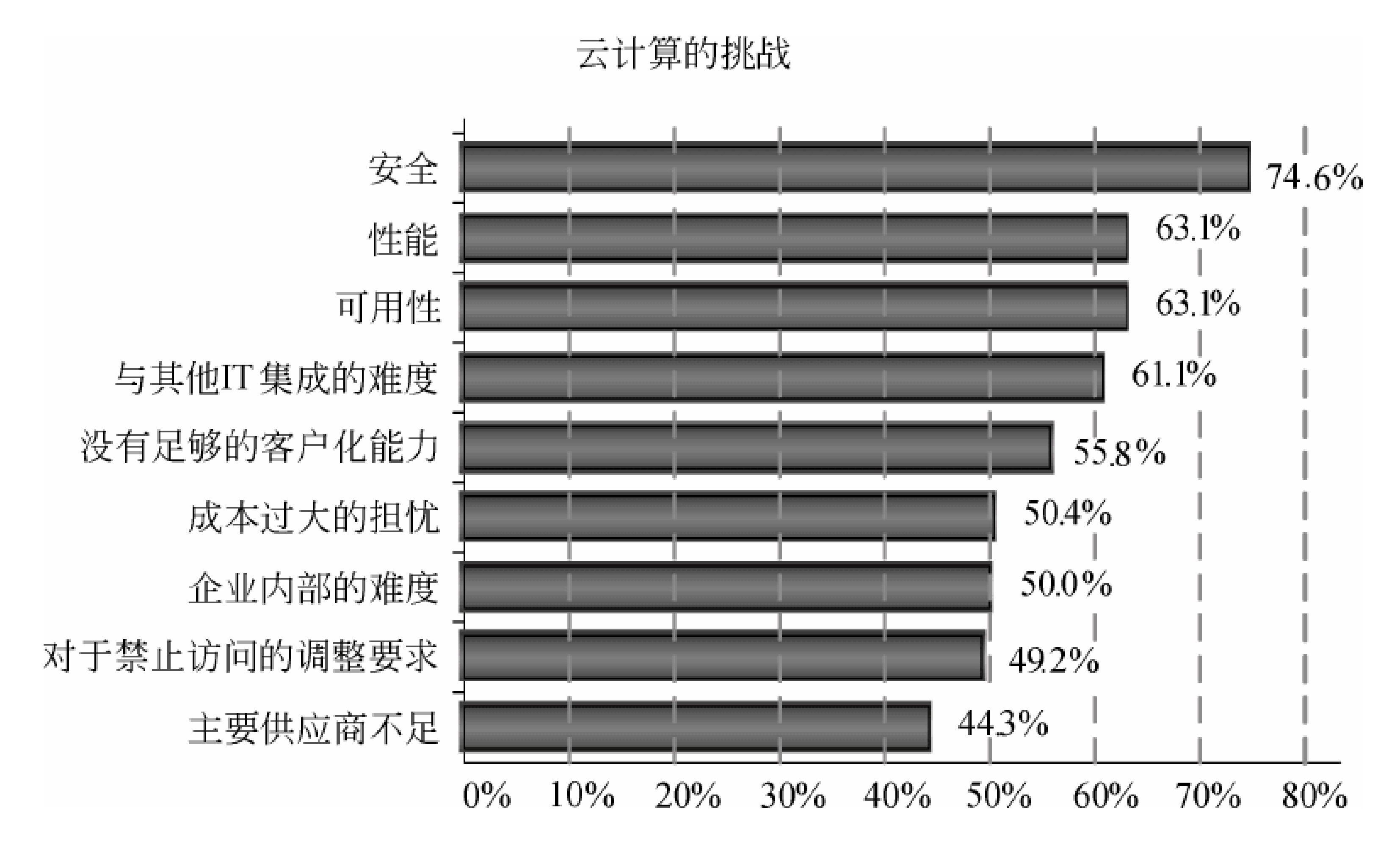


图 5-1 IDC 云计算市场调研情况

2009 年，国际云计算安全联盟 CSA（Cloud Security Alliance）发布了《云计算关键领域安全指南》一文。该文主要讨论了当企业部署云计算系统时面临的安全风险并且给出相应的安全建议。除此之外，还提出了构建云计算安全架构的方法：基于传统的 IT 系统安全控制模型并将其与云服务模型进行一一比对，从中找出安全间隙并加以改进和弥补。文中还分别从云治理和云运行的角度提出了部署云计算系统时需面对的安全“痛点”：治理和企业风险管理、法律与电子证据发现、合规与审计、信息生命周期管理、可移植性和互操作性、传统安全、业务连续性和灾难恢复、数据中心运行、应急响应、通告和补救、应用安全、加密和密钥管理、身份和访问管理、虚拟化。

同年 3 月美国信息系统审计和控制协会 ISACA（Information Systems Audit and Control Association）发布了《Cloud Computing：Business Benefits With security，Governance and Assurance Perspectives》。该文讨论了云计算系统的部署为系统安全所带来的优势和挑战，分析了云计算系统的安全风险和相应的安全建议。该文认为云计算的出现使得传统的网络边界不复存在，使得信息的所有权和管理权分离，在这个环境下对信息的非授权访问是云计算系统的主要安全问题。该文对云计算系统进行了全面的风险评估，并建议将存储在云计算系统中的信息资产根据信息的价值进行合适的归类和标注，为不同价值的信息提供不同等级的安全服务，如存储、传输、加密和审计级别等等。

2010 年，欧洲网络和信息安全中心 ENISA（European Network and Information Security Agency）也发布了云计算安全白皮书。该文认为云计算对于安全有正面也有负面地影响：一方面，在同样的投资额度下，云计算将安全防护资源集中和统一管理，这使得访问控制和安全控制流程更加流畅，比各个企业独立维护的安全防护系统更加全面、稳定；另一方面，云计算系统的使用也会带来很多安全问题，如安全责任分配和管理的缺失、法律法规的缺失、云服务提供商合法合规风险、云计算供应商再选择和信息转移的困难、在多租户场景下用户数据的隔离风险、应用程序接口的脆弱性、数据处理和保护的不透明性。该文提出了云计算系统信息保障安全框架，用来审核云计算系统是否能够满足信息保障的各种安全需求，用户也可以以此为依据评定和选择云计算供应商。

在不同云服务模型中，提供商和用户的安全职责有很大的不同：IaaS 提供商负责解决物理安全、环境安全和虚拟化安全这些安全控制，而用户则负责与 IT 系统（事件）相关的安全控制，包括操作系统、应用和数据；PaaS 提供商负责解决物理安全、环境安全、虚拟化安全和操作系统等安全，而用户则负责应用和数据的安全；SaaS 提供商不仅负责物理和环境安全，还必须解决基础设施、应用和数据相关的安全控制。

5.1.2　从云计算服务模式看安全

不同的云服务模式（IaaS、PaaS、SaaS）的安全关注侧重点不同，IaaS 关注基础设施和虚拟化安全；PaaS 关注平台运行安全；SaaS 关注应用安全等。同时三种云服务模式也有共有的安全问题，如数据安全、加密和密钥管理、身份识别和访问管理、安全事件管理、业务连续性等。

1．IaaS 层安全

IaaS 涵盖了从机房设备到其中的硬件平台等所有基础设施资源层面。IaaS 提供商提供一组 API，允许用户管理基础设施资源以及其他形式的交互。IaaS 层的安全主要包括物理安全、环境安全、主机安全、网络安全、虚拟化安全、接口安全以及共有安全问题等。

物理与环境安全主要包括两个方面：一是保护云计算平台免遭地震、水灾、火灾等事故以及人为行为导致的破坏；二是为云服务提供商的数据中心设施的安全设计和运维进行管理，建立严格的管理规程。

云计算平台的主机包括了服务器、终端/工作站以及安全设备/系统在内的所有计算机设备，主要指它们在操作系统和数据库系统层面的安全。主机安全问题主要包括操作系统本身的缺陷带来的不安全因素（包括身份认证、访问控制、系统漏洞等）、操作系统的安全配置问题、病毒对操作系统的威胁等。

在网络安全方面，主要应该做到以下几方面的安全防护：网络结构安全、

网络访问控制、网络安全审计、边界完整性检测、网络入侵防范、恶意代码防范、网络设备防护。可以采取的主要安全措施和技术包括在网络的边际提供防火墙、防毒墙、入侵检测与防护系统、负载均衡器等安全措施。此处，应特别注意拒绝服务攻击。

虚拟化技术本身引入了 hypervisor 和其他管理模块这些新的攻击层面，但更重要的是虚拟机之间的通信流量对标准的网络控制来说是不可见的，无法对其进行检测和控制，类似这些安全控制功能在虚拟化环境中都需要采用新的形式。还有一个问题是不同敏感度和安全要求的虚拟机（VM）如何共存。

接口安全需要采取相应的措施，来确保接口的强用户认证、加密和访问控制的有效性，避免利用接口对内和对外的攻击，避免利用接口进行云服务的滥用等。

2. PaaS 层安全

PaaS 层的安全，主要包括接口安全、运行安全和共有安全。

对于 PaaS 平台提供的一组 API，需要采取相应的措施，来确保接口的强用户认证、加密和访问控制的有效性，避免利用接口对内和对外的攻击，避免利用接口进行云服务的滥用等。

在 PaaS 上，需要保障用户的 IT 系统的安全部署和安全运行，使其不对现有的 PaaS 平台造成影响和威胁，如不会在云内部发起对内和对外的攻击。运行安全主要包括对用户应用的安全审核、不同应用的监控、不同用户系统的隔离、安全审计等。

3. SaaS 层安全

SaaS 层的安全，主要包括应用安全和共有安全。与传统的操作系统、数据库、C/S 系统的安全漏洞相比，多客户、虚拟化、动态、业务逻辑复杂、用户参与等这些 Web 2.0 和云服务的特点对网络安全意味着巨大的挑战，因此在云计算中对于应用安全，尤其需要注意的是 Web 应用的安全。要保证 SaaS 的应用安全，就要在应用的设计开发之初充分考虑到安全性，应该制定并遵循合适 SaaS 模式的 SDL（安全开发生命周期）规范和流程，从整个生命周期来考虑应用安全。

4. 共有安全

1）数据安全

云服务具有没有位置特异性的特点，这有利于云服务的广泛可用性。然而，无论用户或云供应商或者两者都不可能直接确认在特定云计算资源的详细位置。这就产生了不安全的数据复用问题、数据跨境流动的隐患、用户数据安全和隐私保护等问题。这就对数据存放位置、数据删除或持久性、数据备份与恢复和不同客户数据的混合等方面提出了新的安全要求。

2）加密和密钥管理

加密的机密性和完整性，包括加密网络传输中的数据、加密静止数据、加密备份介质中的数据。云计算中传输加密主要难点在于跨云的数据如何进行传输保护；加密静止数据主要是指加密磁盘上的数据或数据库中的数据，可以防止恶意的云服务提供商、恶意的邻居“租户”及某些类型应用的滥用。对云计算的特殊性而言，应该要求进一步分析加密动态数据的方式，包括内存中的数据。密钥管理包括密钥存储的保护、密钥存储的访问控制、密钥的备份和恢复。

3）身份识别和访问管理

身份识别和访问管理是保证云计算正确运行的关键所在。传统的身份识别和访问管理的范畴，如自动化管理用户账号、用户自助式服务、认证、访问控制、单点登录、职权分离、数据保护、特权用户管理、数据防丢失保护措施和合规报告等，都与云计算息息相关。

在云计算中实施成功有效的身份管理应至少包括：云服务提供商安全和及时地管理创建和更新账户以及删除用户账户；实现跨云的身份认证和管理；身份提供商（IDP）与服务提供商（SP）以安全的方式交换身份属性，实现对身份生命周期的安全管理；建立可信任用户配置文件和规则信息，不但用它来控制在云端服务的访问，而且运行方式符合审计的要求。

4）安全事件管理

对安全事件进行集中管理，实现数据采集、关联分析、事件优先重要性分析、安全事件处理等，从而可以更好地监测发现、评估安全事件，及时有效地对安全事件作出响应，启动适当的措施来预防和降低事件的影响，并从事件中恢复正常的云服务。

5）业务连续性

服务供应商应保证数据中心的运行连续性，保障服务连续性，尤其是在出现一些严重问题时，如火灾、长时间停电以及网络故障等。对于云计算服务提供商而言，就是要进行业务连续性管理，制定相应的业务连续性规划，并且能够得以落实和实施，使得当出现灾难时，可以快速地恢复业务，继续为用户提供服务。

5.2　云计算安全框架

通过上一节我们对 IaaS、PaaS、SaaS 三种云计算服务模式中的安全问题分析，研究提出了云计算平台的安全体系框架，如图 5-2 所示。

对于云计算系统的安全架构的进一步设计，我们建议根据从三个维度去考虑这个问题：安全目标、安全威胁和安全生命周期。首先，安全目标指的是需保护的、可能成为被攻击目标的资产（设备、软件、信息）、行为（登录、登出、数据传输）和流程（管理流程、控制流程等）。对于云计算系统来说，不同的服

务模式涉及的资产、行为和流程各不相同，故而需要根据不同服务模式区分对待，如 SaaS 模式涉及不到任何硬件资产，IaaS 模式涉及不到任何信息资产。其次，安全威胁指的是可以影响、攻击网络目标的事件、手段和方法，如地震、洪水、盗窃、滥用和恶意使用、数据泄露、DDoS/DoS 攻击、病毒、蠕虫等等。在云计算网络中，除了传统的安全威胁以外，也需要对一些新出现的安全威胁和风险付出足够的重视，如数据隔离风险、应用程序接口加固风险、合法合规风险等等。将安全目标（假设 m 个目标）与安全威胁（假设 n 种威胁）合并可以组成了一个 m×n 的矩阵，矩阵的每个结点代表了对某个安全目标的一种威胁，如对网络设备的 DDoS 攻击、对 P2P 应用的滥用等等。安全措施和解决方案将针对矩阵的每个结点中描述的安全风险、问题和攻击。安全架构的最后一个维度称为安全生命周期，它延续了 ISO 27001 的信息系统构建流程“PDCA（plan-do-check-act）”理念。这个维度的主要功能是通过生命周期管理系统去管理和更新安全解决方案，以此来满足不断变化的安全目标和安全威胁。根据这个三维安全架构设计理念，在图 5-2 框架基础上本章进一步提出了一个云计算安全架构，如图 5-3 所示，分别从架构即服务（IaaS）、网络即服务（NaaS）、平台即服务（PaaS）、数据即服务（DaaS）和软件即服务（SaaS）探讨云计算的安全问题、安全威胁和相应的安全解决方案。

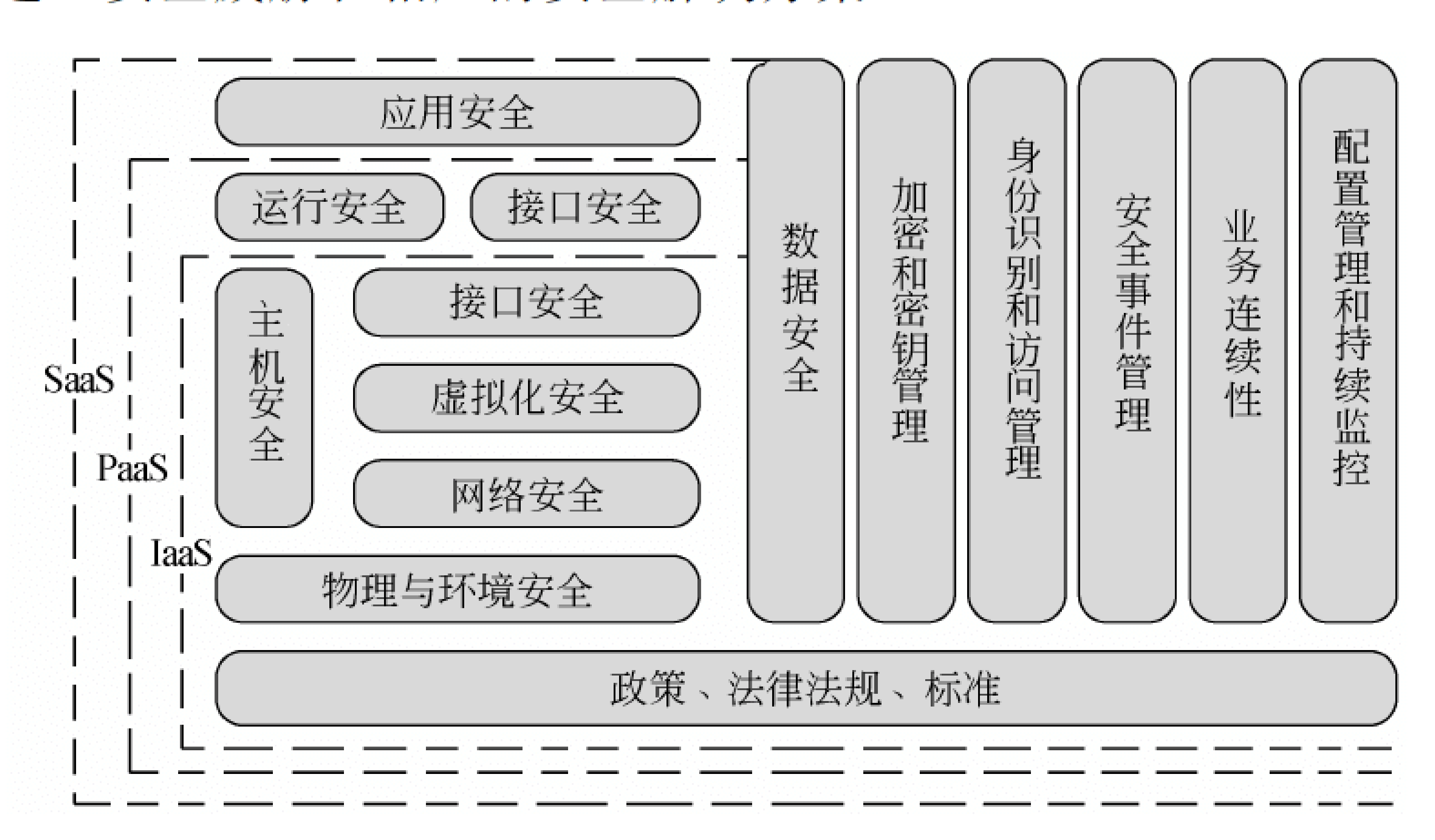


图 5-2 云计算平台的安全体系框架

应用层	SaaS	应用	深度包检验	Web基础防火墙		安全作为一个过程
	DaaS	数据	数据丢失预防	灾难恢复		
运营层	PaaS	运营管理	管理办法，风险管理，规范化管理	虚拟化，数据隔离，访问控制	补丁管理	
基础设施层	NaaS	网络	传输安全	路径监测		
	IaaS	设备	主机基础防火墙，IDS，IPS	系统日志	磁盘加密	
		环境	物理设备安全	录像监控	人工防护	

图 5-3 云计算安全架构

5.2.1 架构即服务（IaaS）

作为云计算基础服务之一，IaaS 旨在为用户提供物理和虚拟的计算存储资源。因此 IaaS 的安全目标往往是保护环境、硬件设备免受各种安全威胁。

1. 物理环境层面

对于 IaaS 云服务提供商来说，他们需提供最基本的安全防护是承载云计算功能的计算和存储设备所处环境的物理安全，包括机房温度、湿度、防洪、抗震，人员访问控制、防盗、视频监控和人力安保措施。这些防护措施的目的与目前计算机系统的通用安全措施是一致的，旨在保护计算机所在环境的基本安全、保证计算机的基本运行条件以及阻止因为外界环境的变化对计算机运行带来的负面影响。

2. 主机层面

从物理层面上看，云计算系统是由一个又一个的处在不同位置的网络计算单元和存储单元有机结合而成的。因此每个计算单元和存储单元需根据具体需求配备一定基于主机层面的安全功能。其中，包括基于主机的防火墙、基于主机的入侵检测系统、基于主机的入侵防护系统、磁盘加密管理系统等来完成主机保护功能；还包括硬件/软件日志管理系统和相应的安全事件响应管理来完成审计功能。这些安全措施和系统通过保护单个主机形成了云计算系统的第一道防线。

5.2.2 网络即服务（NaaS）

网络在云计算系统中起到的作用是为处于不同位置的计算单元和存储单元提供稳定、安全、保密的连通功能。在很多情况下，这些计算单元和存储单元往往位于不同的网络域之中和防火墙之后。也就是说，这些结点之间是无法直接互访的。NaaS 提供的功能就是将传统的网络边界打破，直接连接云结点并生成云的混沌架构。当然，保证连通的稳定性、安全性和机密性也是 NaaS 服务商的主要责任之一。

1. 传输的安全性

在云计算系统中，计算结点之间的互联互通往往会跨越非安全的公共网络，因此数据传输面临着窃听、篡改、损毁等各种风险。从原理上说，若要保证数据传输的安全则需要保证在发包端、收包端和包传输全过程三方面的安全。对于发包和收包的终端来说，可以通过基于终端的安全措施来保护数据传输在发送和接收过程中的安全性，如安全输入输出、内存屏蔽、存储密封等。云计算系统中结点之间的安全数据传输可以通过加密隧道技术保证数据传输的机密

性，通过数字摘要、数字证书和数字时间标签来保证数据的完整性和不可篡改性。

2. 流量监控

流量监控旨在监测和控制云计算结点之间的流量特征，实时发现异常流量并加以管理和控制。对于流量“异常”的定义往往需要将某一区域或链路大部分时间的流量统计数据作为基准。当某一时刻这个链路或者区域的流量特征与这个统计值有非常大的出入时，就会被认定为“异常”场景。在云计算系统中，当文件和数据被分割、存储在多个虚拟机上之后，它们往往很少被再次移动了，因为那会耗费很多不必要的网络传输资源。所有的计算命令将以并行计算的方式发布到各个数据碎片上，数据处理完成后只传回处理结果，这个工作模式即计算向存储迁移。因此，云计算系统结点之间的通信对大数据量传输往往非常谨慎，并且对异常流量非常的敏感，如洪水攻击、蠕虫等等。流量监控往往牵涉到从网络 IP 层到应用层的多种技术，在云计算的架构层，可以使用基于数据包和数据流的流量分析和控制工具加以实现，如五元组分析工具、基于 Netflow 的流分析等等。

5.2.3 平台即服务（PaaS）

我们可以用一个非常形象的比喻来说明云计算平台：它就像是运行在传统计算机上面的操作系统，只不过这个操作系统有些特殊，它运行在互联网和多台虚拟机上，它将互联网上的多台计算机、服务器、存储器变成了一个网络计算机。云计算平台是云计算产业的核心技术，目前只有少数几家公司有能力开发商用云计算平台。从安全的角度来看，这个平台需要有能力保护云计算系统中存储的数据、传输命令和计算结果、管理用户鉴权和访问控制。

1. 虚拟化和数据隔离

从云计算平台的角度来看，云计算系统最基本的单元是虚拟机。当一个文件初次存储到云计算系统中时，它会被分割成若干个碎片并存储在不同的虚拟机上，并在各个虚拟机上面并行地完成对文件碎片的操作。这个文件分割、存储和计算管理的全流程都是由云计算平台来负责的。来自不同公司的重要信息和文件可能会被存储在同一个虚拟机上，因此数据隔离和数据保护就显得非常重要了。虚拟机本身往往会附带一系列的数据管理系统，可以实现一定的加密、数据访问控制和数据隔离功能。除此之外，虚拟防火墙可以实现针对单个虚拟机设置安全策略和访问控制策略。最后，云计算系统中的虚拟机可以被分成若干组，并配置不同的安全级别，如不同的加密强度、数据备份、数据恢复设置。用户数据在初次存储到云计算系统中的时候，系统可以根据用户的服务级别将用户数据存储在不同的虚拟机组中以实现服务分级和安全保护分级。

2．补丁和设置管理

在云计算行业中，目前有几款已经发布的云计算平台产品，包括商用产品如亚马逊的 EC2/S3 平台、谷歌的 App Engine 平台、微软的 Azure 平台，以及开源产品如 Hadoop、Eucalyptus、Enomaly ECP、Nimbus、Abiquo 等。从本质上说，云计算平台是一种软件操作系统，所以 PaaS 平台也需要完善的补丁和设置管理系统及流程去不断地完善云计算平台以应对不断出现的安全威胁和新发现的系统漏洞。

3．治理、风险和合法合归管理

传统的治理、风险和合法合归（GRC）管理平台几乎是伴随萨班斯-奥克斯利法案（Sarbanes-Oxley Act，SOX）的生效而在世界范围内风靡的，尤其在北美。治理、风险和合法合归管理平台旨在帮助行业和企业用户去跟踪项目进程、管理风险并遵从不同国家和地区的法律法规的需求。但是在云计算系统中，传统的 GRC 平台已经不再适合云计算的特点了，而是将 GRC 功能集成到云计算平台上。在另一方面，由于往往会有多种行业的用户使用同一云计算平台，因此集成在云计算平台上的 GRC 系统需要同时满足不同企业在治理、风险和合法合归方面的特点和需求，并且细化到为用户（企业）提供“法律遵从”的文件管理流程、工作流程，或提供商业法规资料库等。

5.2.4　数据即服务（DaaS）

DaaS 泛指云存储服务，它可以部署在 PaaS 平台之上，也可以直接部署在 NaaS 和 IaaS 之上。但无论是哪一种部署方式，DaaS 平台的部署都会牵涉到存储阵列的部署和相应的管理软件的加载。对于 DaaS 来说，它面临的安全威胁主要是来自数据方面的，主要包括防数据外泄管理和灾难恢复。

1．防数据外泄管理

云计算系统的防数据外泄管理（DLP）旨在保护存储在云计算系统中的客户数据以防来自内部和外部的非授权的访问和传输。当有竞争关系的多个企业用户将各自公司的机密数据存储在同一个云计算服务提供商的网络上时，数据泄露威胁就变得尤为突出了。对于用户来说，云计算系统的数据处理是非透明的，即用户并无法获知云计算系统将其资料存储的具体位置，数据读取的流程和路径是什么，哪个虚拟机在处理它，如何处理它。换句话说，用户无法对其重要文件和数据保持有效的机密控制。但是这些数据的存储、读取、管理等诸多流程对于云计算服务提供商来说是透明的。在这种情况下，云计算服务提供商就需要负担起保护存储在云计算系统中的所有数据的责任，并根据各用户的具体需求建立一个完备的 DLP 系统规范包括自己在内的各个公司员工的行为，

保证各个公司的机密数据不被外泄。总体来说，云计算的 DLP 需要完成两个主要的目标：防止来自企业用户外部的数据窃取和防止来自企业用户内部的数据泄露。来自企业用户外部的数据窃取可以通过云计算平台的用户授权、访问管理和数据加密来保护。防止来自企业用户内部数据泄露的主要措施有深度内容检测和行为检测：深度内容检测可以确定数据的重要性并确保其自动转移到安全级别较高的磁盘空间上；行为检测则是通过监控员工对数据的操作并作出如允许、拒绝、警告的响应。

2. 灾难恢复

数据备份和灾难恢复是指将系统关键状态、日志和用户数据进行周期性备份，以备系统在遭受了自然或人为灾害后，重新启用系统的数据、硬件及软件设备，恢复正常商业运作。由于云计算系统是广泛分布在不同地理位置的计算单元和存储单元的集合体，故而它在灾难恢复上有着先天的优势。它的难点在于在同一云计算系统中根据不同行业企业的业务特点和恢复需求规划不同的灾备计划和系统，包括对企业或机构的灾难性风险作出评估，对关键性业务数据、流程予以及时记录、备份，设置不同的业务恢复时间和业务恢复点。

5.2.5 软件即服务（SaaS）

SaaS 提供商借助应用程序接口将云计算软件部署在云计算平台之上。这些云计算软件可以为某个或多个行业提供服务，如流程管理、订单管理、客户管理、企业内部管理等。由于用户拥有极其有限的权限对云软件进行二次开发，所以在 SaaS 模式下的安全责任基本由云服务提供商负担。

1. 深度包检测

在一些特殊的场景下，一些云计算应用非常有可能被滥用和恶意使用：云计算系统强大的计算能力和网络能力有可能会被用作 DDoS 攻击、垃圾邮件发送、非法暴力破解密码。这些现象的出现需要云计算服务提供商准确地了解谁使用什么应用、在如何使用它的服务和资源。深度包检测技术在应用识别方面拥有得天独厚的优势。深度包检测技术不但分析数据包的包头，还通过模式识别、行为分析和统计分析等算法分析数据包的载荷。对于网络第三层的数据包来说，它的载荷包括了有效载荷和第四层至第七层每一层的包头信息。换句话说，深度包检测技术对网络流量的分析覆盖了从第三层到第七层的全方位分析。若将深度包检测技术应用到云计算系统中，它能够使得云计算系统准确地了解到应用正在被谁使用、如何使用。

2. Web 应用程序防火墙

云计算软件服务提供商通过基于 Web 的“瘦”客户端为用户提供鉴权、登

录和应用是云计算软件服务非常常见的场景。但由于 Web 浏览器本身的脆弱性，Web 应用程序会很容易被植入恶意代码而对用户和服务提供商带来损失。Web 应用程序防火墙可以良好地防范一些基于 Web 的常见攻击，如跨网站脚本攻击、SQL 注入等。

5.2.6　安全是一个过程

为云计算系统设计安全架构是一个长期和全面的过程。在 ISO 27001 构建信息安全管理系统的“Plan-Do-Check-Act（PDCA）”流程的启发下，我们提出：云计算安全系统和框架不是通过上马一个产品、一种解决方案或者一套流程规范可以实现的，它是一个长期的并且不断完善的过程，即安全是一个过程。首先，云计算服务提供商需定义所属系统的资产（物理和信息资产）、安全需求和安全计划并以此定义相应的安全控制策略。在不同的云计算服务模式下，资产是各不相同的：SaaS 和 PaaS 提供商拥有的资产仅涵盖软件和数据，安全控制需面向信息安全和平台稳定；对于 IaaS、NaaS 和 DaaS 模式，资产既包括信息资产还包括物理资产，安全控制策略需将物理环境安全囊括在内。其次，安全策略需根据资产的变更、安全需求的提升或降低来周期性地检查和更新现有的安全控制策略。

5.3　云计算安全标准化现状

5.3.1　国际和国外标准化组织

1. ISO/IEC JTCI SC27

ISO/IEC JTCI/SC27（信息安全分技术委员会）于 2010 年 10 月启动了研究项目《云计算安全和隐私》，由 WG1/WG4/WG5 联合开展。目前，SC27 已基本确定了云计算安全和隐私的概念体系架构，包括八方面内容：①概念、定义；②安全管理要求；③安全管理控制措施；④安全技术；⑤身份管理和隐私技术；⑥审计；⑦治理；⑧参考文件。基于该架构，明确了 SC27 关于云计算安全和隐私标准研究的三个领域：

（1）ISO/IEC 270xx（信息安全管理）：由 WG1 负责研制。标准项目主要涉及要求、控制措施、审计和治理。项目编号目前确定为 ISO/IEC 27017。其中的第 2 部分（即 ISO/IEC 27017-2）是目前 SC27 唯一一个云计算安全标准项目《基于 ISO/IEC 27002 的云计算服务使用的信息安全管理指南》（标准类型属技术规范）。该项目是基于日本提案而产生的，目前已经形成工作草案文本。按照工作进度，将于 2013 年底正式发布。

（2）ISO/IEC 270yy（安全技术）：由 WG4 负责研制。它主要基于现有的信息安全服务和控制方面的标准成果，以及必要时专门制定相关云计算安全服务和控制标准。

（3）ISO/IEC 270zz（身份管理和隐私技术）：由 WG5 负责研制。它主要基于现有的身份管理和隐私方面的标准成果，以及必要时专门制定相关云计算隐私标准。

2. ITU-T

国际电信联盟通信局于2010年6月成立了ITU-T云计算焦点组，主要致力于电信方面的研究，如电信方面的安全和管理，目前在安全方面的输出物为《云安全》。焦点组的运行时间是截止至 2011 年 12 月，后续工作已经分散到别的 SG（研究组）。近日，在 SG13（下一代网络）成立了云计算工作组，该组将负责输出ITU-T推荐的关于云服务互操作性、云数据可移植性的多项标准。安全方面主要由 SG17（安全）承担，工作范围集中在框架和需求等方面。

3. CSA

云安全联盟（CSA）是在 2009 年的 RSA 大会上宣布成立的，目的是为了在云计算环境下提供最佳的安全方案。目前的成果有：《云计算关键领域安全指南》、《云计算的主要风险》、《云安全联盟的云控制矩阵》、《身份管理和访问控制指南》。CSA 已经与 ITU-T、ISO 等建立起定期的技术交流机制，相互通报并吸收各自在云安全方面的成果和进展。CSA 目前所进行的工作主要是研究，所有的成果以研究报告的形式发布，并没有制定标准。

4. ENISA

欧洲网络与信息安全局（ENISA）目前发布了三本白皮书：《云计算中信息安全的优势、风险和建议》、《政府云的安全和弹性》、《云计算信息保证框架》。在《政府云的安全和弹性》中，对于政府部门提出了四点建议：①分布分阶段进行，因为云计算环境比较复杂，可能会带来一些没有预料到的问题；②制定云计算策略，包括安全和弹性方面，该策略应该能够指导 10 年内的工作；③应该研究在保护国家关键基础设施方面，云能够发挥的作用、扮演的角色；④建议在法律法规、安全策略方面做进一步研究和调查。

5. NIST

2010 年 11 月，美国国家标准技术研究院（NIST）云计算计划正式启用，该计划旨在支持联邦政府采用云计算来替代或加强传统信息系统和应用模式。由美国联邦政府支持，NIST 进行了大量的标准化工作，它提出的云计算定义被许多人当成云计算的标准定义。NIST 专注于为美国联邦政府提供云架构以及相关的安全和部署策略，包括制定云标准、云接口、云集成和云应用开发接

口等。目前已经发布了多份出版物，如下：

SP800-144《公共云中的安全和隐私指南》、SP800-146《云计算梗概和建议》、SP500-291《云计算标准路线图》、SP800-145《云计算定义》、SP500-292《云计算参考体系架构》、SP500-293《美国政府云计算技术路线图》。此外，NIST 还发布了其他输出物：《云计算安全障碍和缓解措施列表》、《美国联邦政府使用云计算的安全需求》、《联邦政府云指南》、《美国政府云计算安全评估与授权的建议》等。

6．其他

分布式管理任务组（DMTF）已经发布了 OVF（开放虚拟化格式）1.0，目前正在制定 OVF 2.0，以解决虚拟云计算环境中出现的管理和互操作性问题；结构化信息标准促进组织（OASIS）发布了《云计算使用案例中的身份管理》，制定了加密客户端和密钥管理服务器之间的通信协议的 KMIP，并得到 IEE SISWG 和 CSA 的认可；全球网络存储工业协会（SNIA）制定了一套云存储系统管理接口《云数据管理接口规范 CDMI 1.0》，已经通过了 NIST SAJACC 使用案例的初次测试。

5.3.2　国内标准化组织

目前全国信息安全标准化委员会（TC260）在开展云计算安全方面的研究，承担了多项云计算安全相关的项目，在信安标委内部设立了专门对云计算及安全进行研究的课题，并于 2011 年 9 月完成《云计算安全及标准研究报告 V1.0》。目前正在研究的标准项目为《政府部门云计算安全》和《基于云计算的因特网数据中心安全指南》等。

云计算安全联盟（CSA）成立中国区分会，分会继承 CSA 的宗旨和目标，致力于提升中国（含港澳台地区）的云安全实践，为世界范围内以汉语为主要沟通语言的专家和专业人士进行社区分享、协作和共同开发，增进与国际同行的交流等作出贡献。2009 年 12 月 17 日，云安全联盟发布了新版的《云安全指南》，另外开展的云安全威胁、云安全控制矩阵、云安全度量等研究项目在业界得到积极的参与和支持。2011 年，CSA 推出了若干个重要项目，包括云安全指南新版本 3.0、云安全事件响应 CloudSIRT、CSA 知识认证 CCSK、CSA Governance Stack、CSA STAR 计划等。

5.4　云计算安全解决方案概述

云计算安全框架从宏观的角度描述了企业部署云计算需要考虑的层面、角

度，它囊括了一个全面的保证云计算安全的技术沙盘。实际上，在企业的真实部署中是不可能将沙盘中所有的安全技术都使用起来，它们有的功能重复、有的甚至相互冲突。在产业界，很多大型公司围绕着一两样云计算安全关键技术衍生出一整套安全解决方案，下面将举例说明。

5.4.1 亚马逊云计算安全解决方案

亚马逊云计算安全解决方案致力于合法合规、网络安全、安全管理、虚拟化安全、数据安全等多方面的研究，如图 5-4 所示。法律法规：符合 SOX（财务领域）法案和 SAS70 Type II 审计框架，AWS 的用户在 S3 上构筑了符合 HIPAA（医药行业）的应用。网络安全：防范 DoS/DDoS 攻击、MITM 攻击、IP Spoofing、Port Scan 攻击、安全组隔离，客户可以自定义安全组。VPC，用户创建 VPC 连接已有的用户网络，VPC 之间可以相互隔离。安全管理：在 EC2 业务中，AWS 的管理员必须使用强 SSL 密钥（X.509 证书）访问主机，管理员没有 Guest OS 的管理权限。用户拥有用户操作系统的所有管理权限，通过基于 token 的或者密钥的 SSH 访问虚拟机。虚拟化安全：VM 间安全隔离，VM 没有访问硬件的权限。数据安全：simpleDB 与 S3 都支持用户加密数据上传。

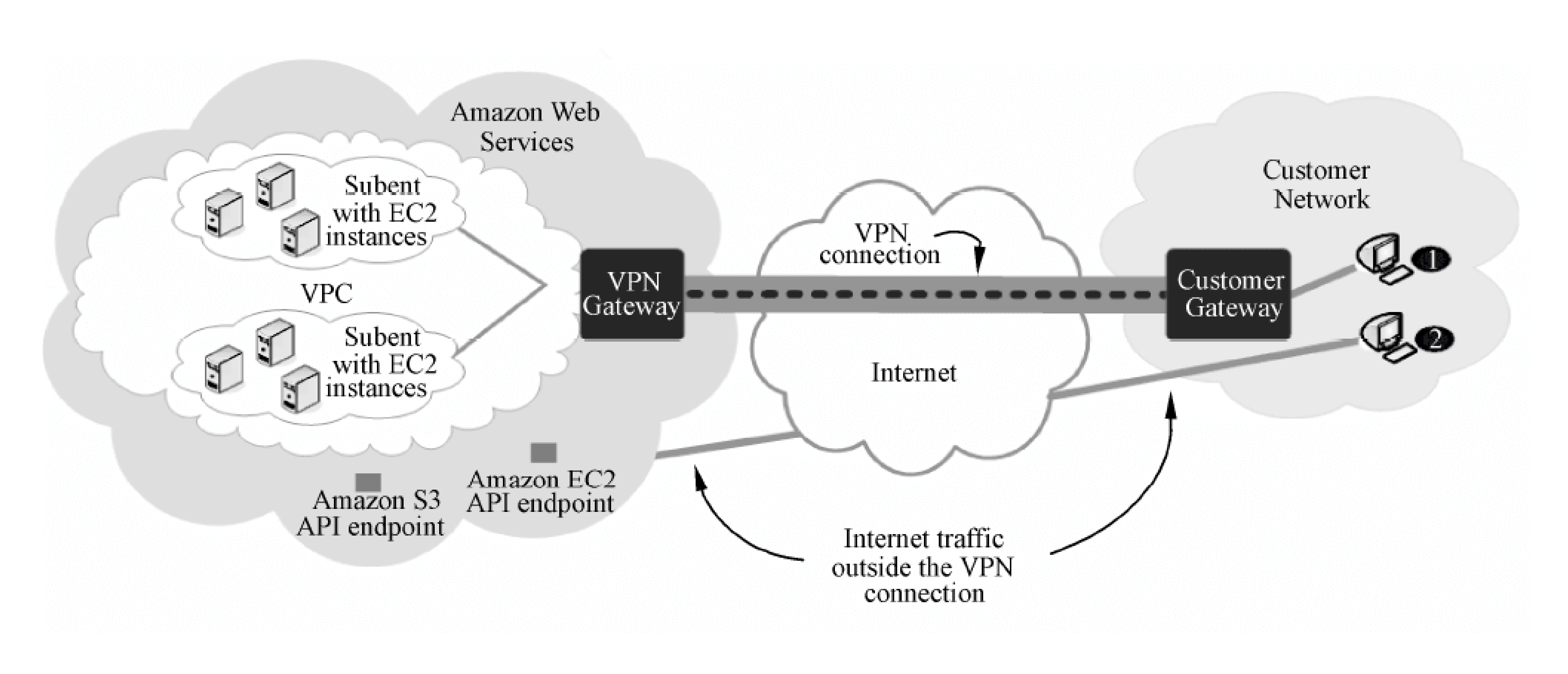


图 5-4 亚马逊云计算安全解决方案

5.4.2 IBM 虚拟化安全 sHype 解决方案

IBM sHype（安全 Hypervisor）的主要功能在于完善虚拟机间信息流的控制，是 Hypervisor 完成资源隔离的增强。它包括在多分区间进行强隔离保证，不同分区间的共享被有效控制，平台与分区的完整性保护，平台与分区的内容验证，资源计算与控制，如图 5-5 所示。

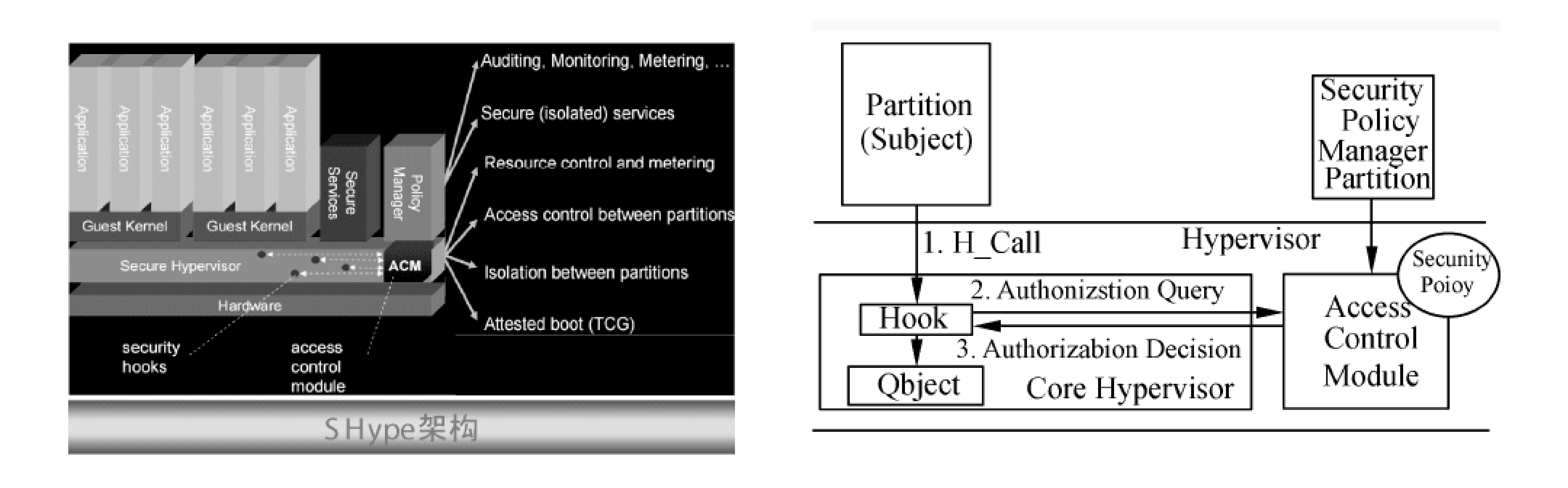


图 5-5　IBM SHype 云计算安全解决方案

5.4.3　IBM 基于 XEN 的可信虚拟域（TVD）

如图 5-6 所示，IBM 通过将可信计算模块虚拟化，将可信计算技术应用到虚拟领域中。IBM 虚拟可信计算方案主要包括：①VTPM 技术，它将硬件 TPM 虚拟化，每个虚拟化的 VTPM 可以保护每个虚拟机的安全性；②TVD 可信虚拟域技术，它实现各虚拟域的信任关系建立的功能。

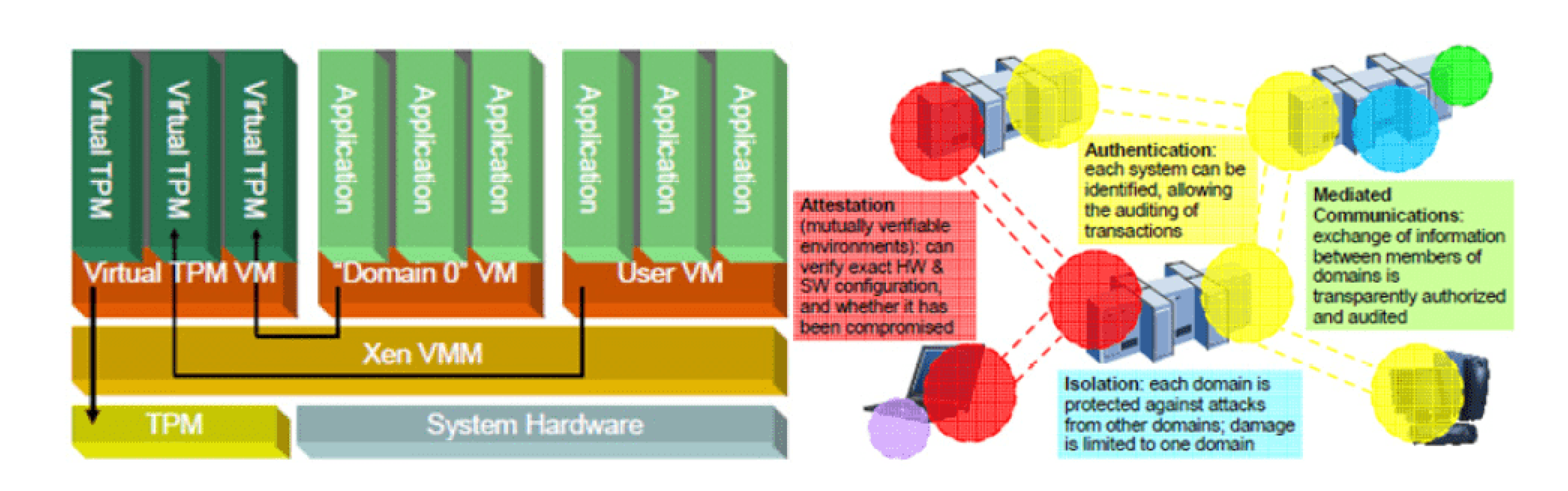


图 5-6　IBM 可信虚拟域技术

5.4.4　VMware 虚拟化安全 VMSafe

如图 5-7 所示，VMSafe 解决方案包括三个功能：AntiVirus、Inter-VM 流量控制、VMsafe 安全状态和策略。AntiVirus VMsafe 为第三方安全厂商通过 VMSafe 提供的 API 提供一个单独的 VM 对所有其他 VM 进行病毒防护，避免每个 VM 安装防病毒代理，并可以对在线与离线的 VM 进行文件扫描杀毒；Inter-VM 流量控制监控与控制所有 VM 的网络活动，每个 VM 有自定义的网络安全策略，监控多个网络，避免安全瓶颈；VMsafe 安全状态和策略在 Vmotion 时可以动态迁移，确保持续的不丢失状态保护。

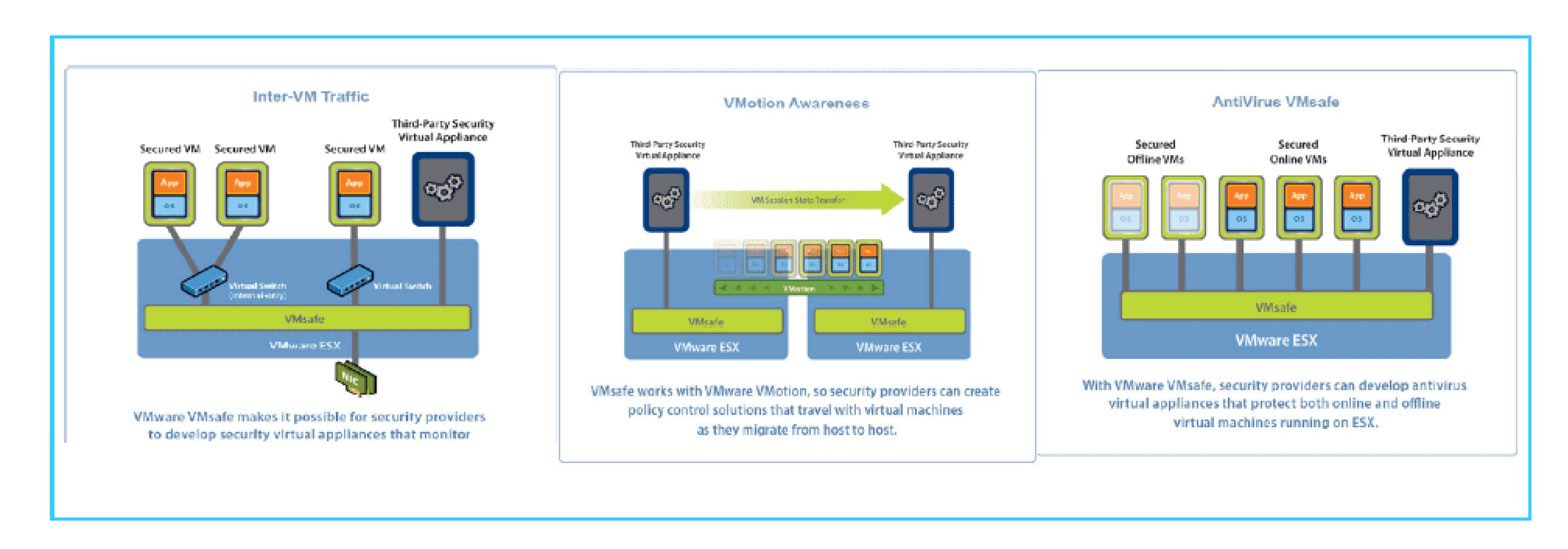


图 5-7 VMSafe 虚拟机安全方案

5.4.5 Cisco 云数据中心安全解决方案

Cisco 安全的优势集中在网络安全上，比如网络设备支持 VPN，有完善的防火墙、IPS 等设备。Cisco 在网络 VPN 技术的基础上，通过引入 VDC（Virutal Device Context）平面隔离功能，将一个物理交换机虚拟成多个虚拟交换机，虚拟交换机完成各虚拟机之间的安全隔离，如图 5-8 所示。Cisco 还可以支持安全策略跟随虚拟机的迁移。

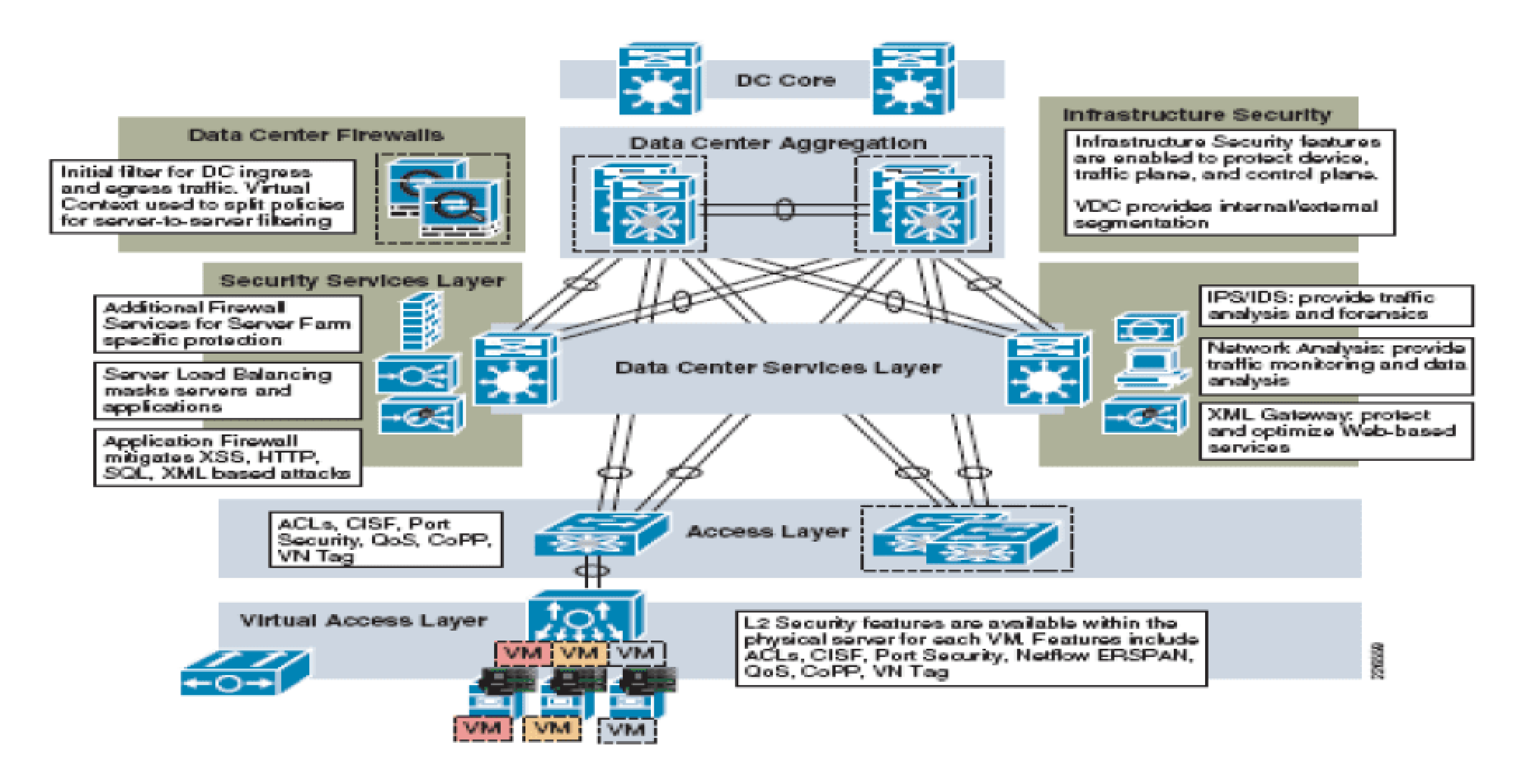


图 5-8 Cisco 云计算数据中心安全解决方案

5.4.6 华为云安全解决方案

华为云计算安全解决方案是一个囊括了设备安全、网络安全、管理安全和数据安全的全方位云计算安全体系。

1. 设备安全

云计算设备安全关注物理层单个设备的安全，实际上它与传统的安全并没

有什么不同。设备级的安全是整个云计算安全最基础的部分。设想云计算系统中的一些基础设备，如服务器、虚拟交换机等因为安全漏洞被黑客渗透，那么无论网络、平台、管理等上层安全做的如何出色，整个系统都没有任何安全性可言。华为在设备层通过咨询服务的方式为用户提供系统加固和集中补丁管理服务。

系统加固服务指的是在业务结点、管理结点和用户/管理 Portal 等不同组件采取业界和华为的安全工具来实现系统加固，保证基础设施的安全性。

集中补丁管理通过快速有效的安全补丁集中管理策略，及时保障云平台各组件的安全。它包括以下几个步骤：集中安全补丁管理，由补丁服务器分发补丁和策略控制；根据补丁策略，各结点自动完成补丁安装；结合虚拟机迁移控制，保证物理机器重启不中断业务；安全补丁按严重程度等级管理，保证紧急、严重补丁能及时安装到现网。

2. 网络安全

网络层面的安全是云计算系统急需考虑的问题。在网络层面，由于虚拟化技术的广泛应用，传统的网络边界不复存在。所以，基于物理边界防护的安全技术在云计算系统中无法适用了，我们需要基于虚拟网络的技术和安全方案。

如图 5-9 所示，在云计算虚拟化系统中，人们第一想到的是通过 VLAN 技术保证云计算虚拟域的隔离。通过划分不同的 VLAN，将计算、管理、存储三个平面进行隔离。诚然，这种技术是可行的，但是它的缺陷也是明显的：VLAN 无法动态设置。也就是说每当虚拟机产生漂移的时候，VLAN 无法将虚拟机的安全策略随漂移而动。在这个方面，我们需要更灵活的解决方案来实现。

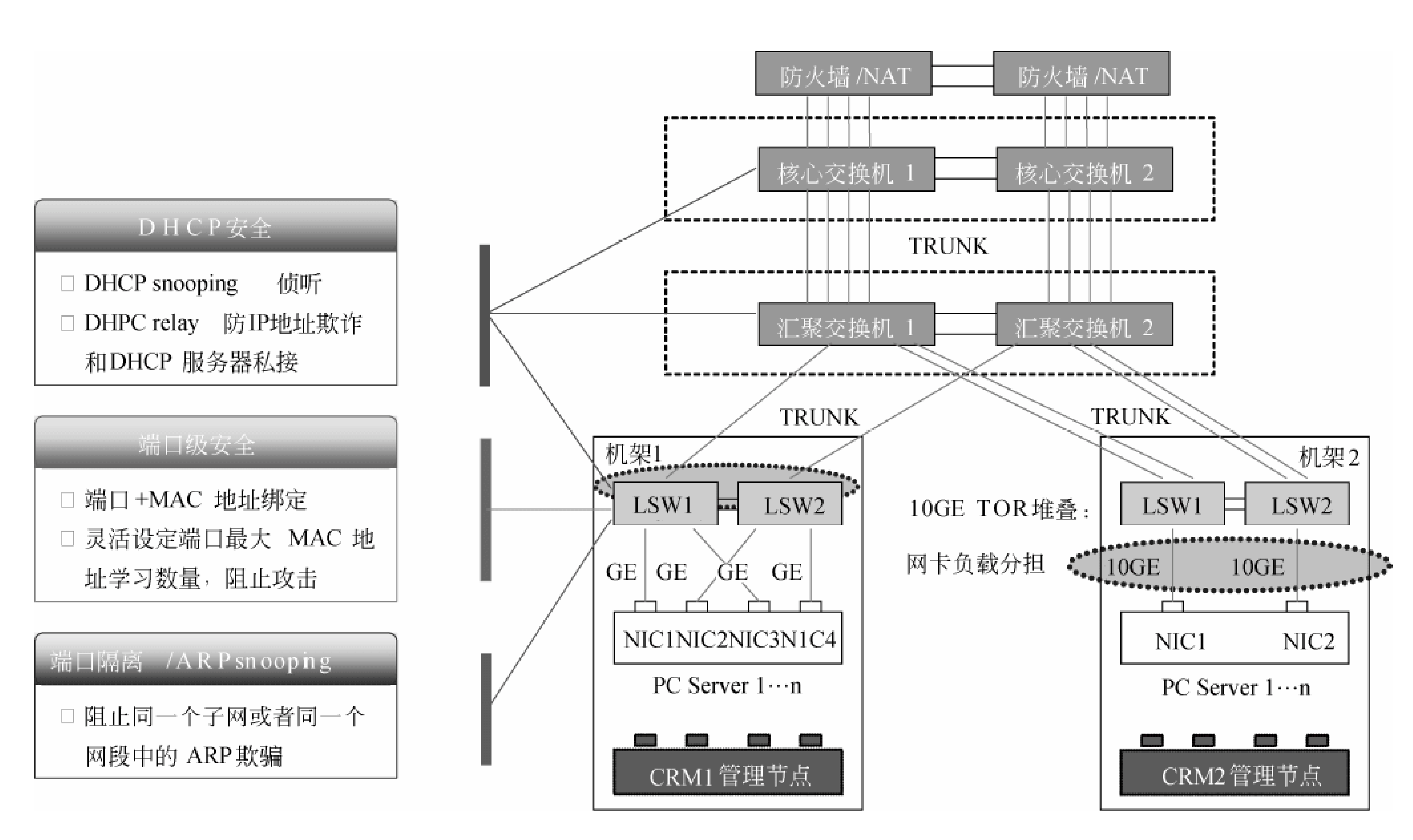


图 5-9　华为虚拟化网络安全

3．虚拟化安全

云计算虚拟化安全是云计算安全区别于其他安全需求的核心特征之一。云计算是运行在多台物理机虚拟出来的虚拟机集群上的，通过对虚拟机集群的管理、任务的集中分配、动态调整提高效率。换句话说，虚拟机之间的通信、交互是云计算存在的基础，但是虚拟机之间的隔离又是其安全的核心诉求。这一对矛盾需要妥善的解决。

华为云计算虚拟化安全为虚拟机集群提供安全组解决方案。如图 5-10 所示，安全组为用户提供安全、可靠的隔离策略，确保只有授权的访问才被接受，防止恶意 VM 的访问。

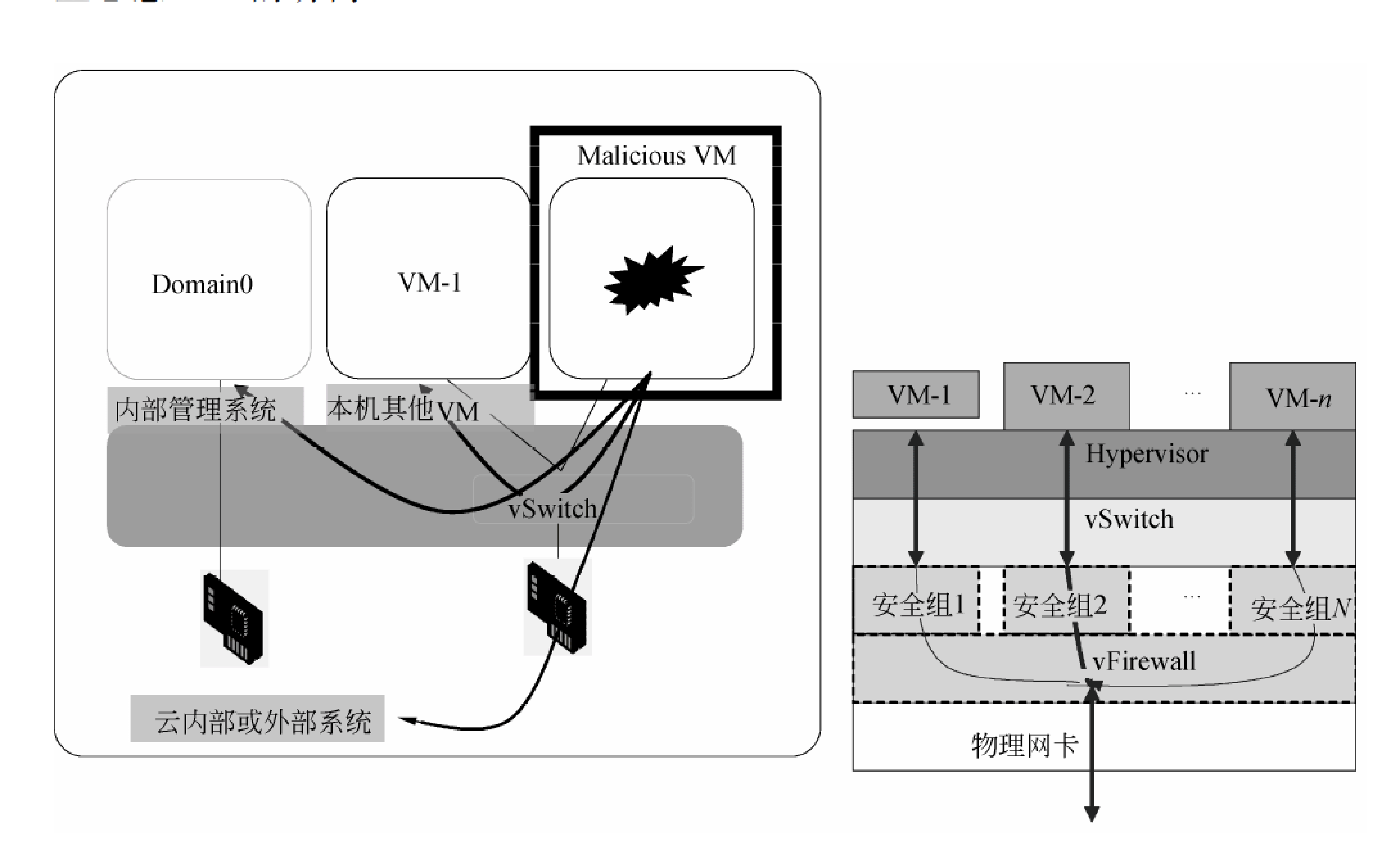


图 5-10 华为虚拟机安全组策略

安全组支持 IP 地址与 MAC 地址绑定、MAC 地址与 VM 绑定，VM 只能发送本机 IP 地址和 MAC 地址的报文；发给某个 VM 的数据包会被 vSwitch 从特定的虚拟端口送出，其他 VM 不能嗅探。检测到僵尸网络可发送信息客户，或通知管理员手动采取措施。

4．管理安全——用户统一身份认证

如图 5-11 所示，华为用户统一身份认证方案支持多因素认证，确保用户、终端的私密性。可使用电信级安全接入控制网关、802.1x 或主机防火墙方案，部署于 L3 或 L2，满足复杂网络需求；通过丰富的安全策略，主动降低终端安全威胁，保障员工合理利用网络资源；基于自动化部署，有效降低您的实施成本与复杂性。

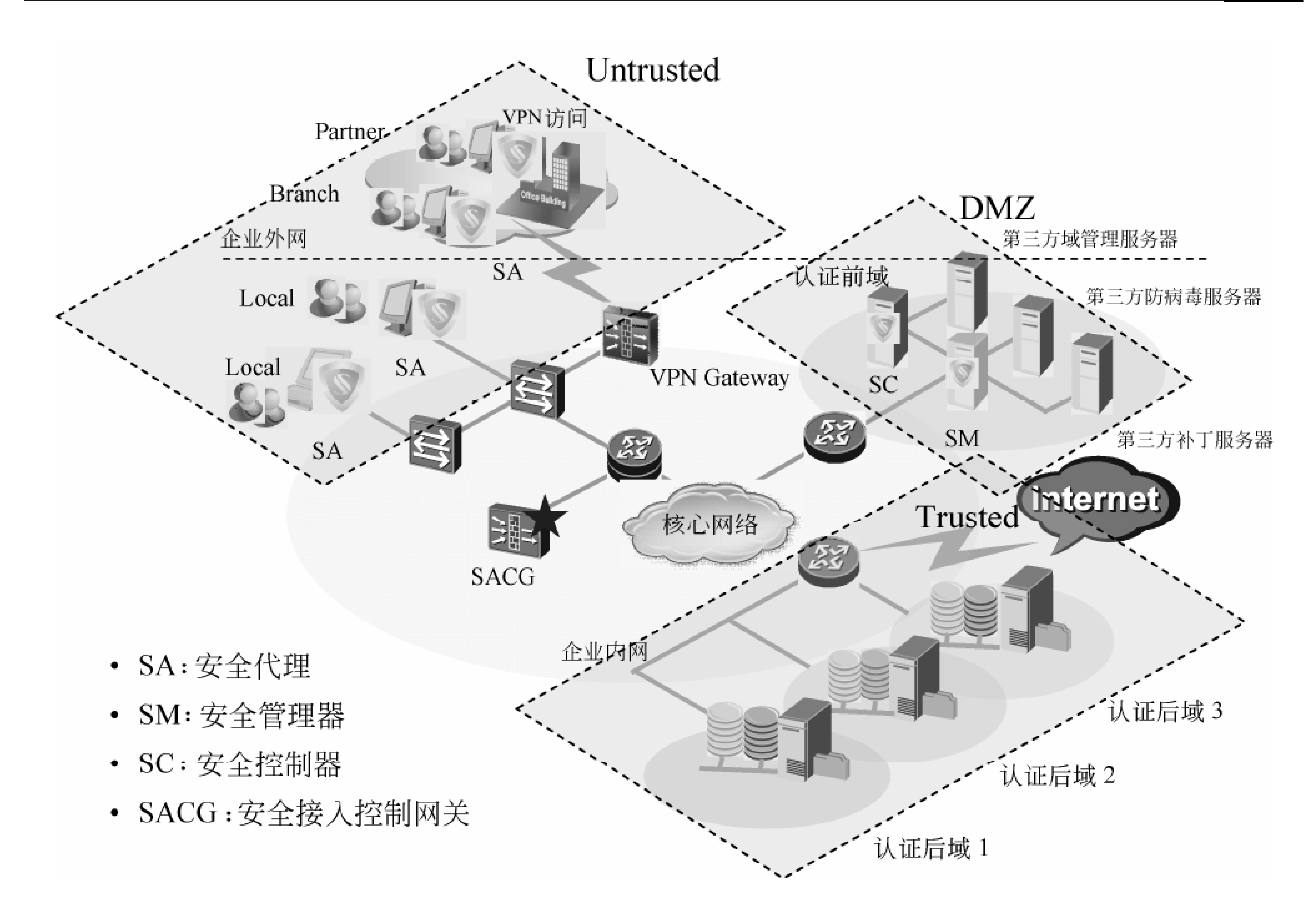
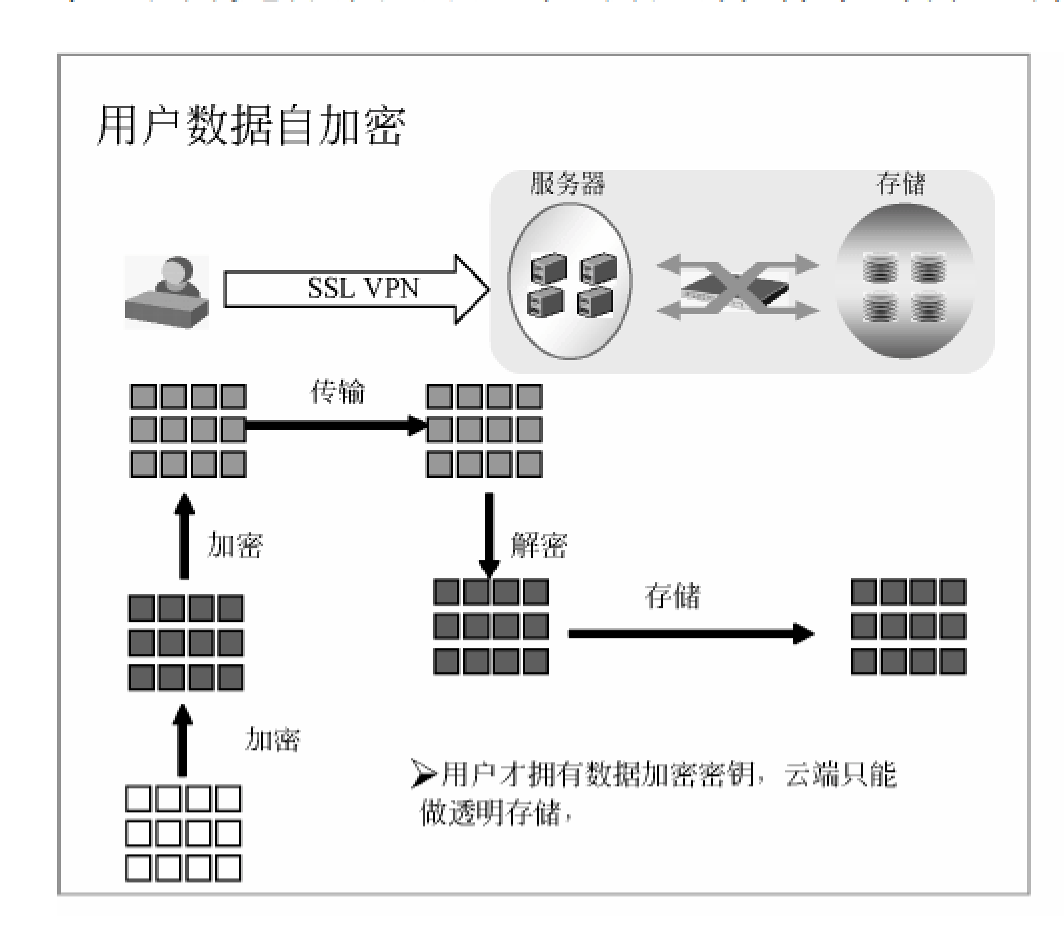


图 5-11 华为用户统一认证解决方案

5. 数据安全

用户数据自加密方案只能用于数据的透明存储。在云端对数据加密采用对称式加密算法确保加密的速度，支持多种加密算法，如 DES、3DES、AES、SM1，SM2 等。数据加密由云端完成，密钥以加密的形式保存在云端，只有虚拟机的用户才有数据密钥的私钥。加密的数据密钥在 TC 端完成解密后，通过安全 SSL 传输到云端对数据进行解密，解密的数据密钥不保存。数据密钥通过用户的证书公钥完成加密，私钥只保存在客户端，不在网上传输，如图 5-12 所示。



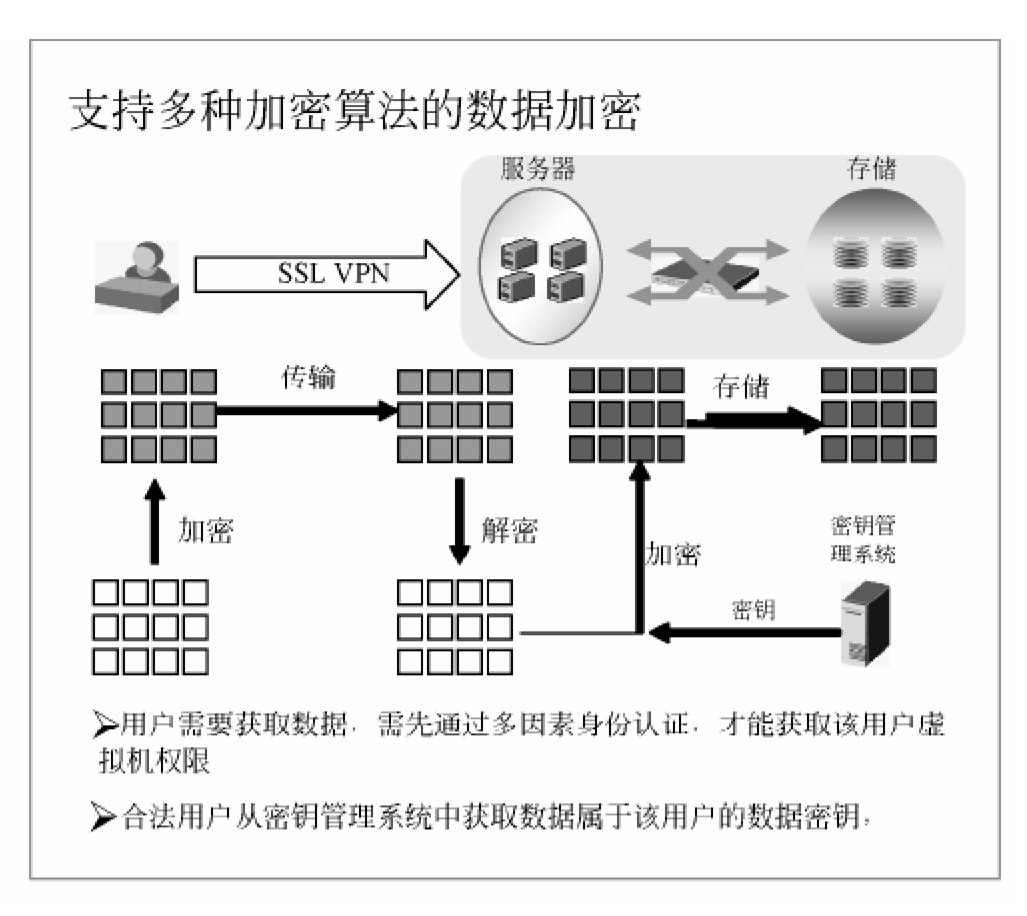


图 5-12 华为云数据安全

5.5 云计算安全开放命题

目前，云计算领域尚有一系列的问题有待探讨和妥善解决。

1. 隐私管理

多个云计算风险评估报告中都指出，缺乏隐私管理是阻止用户使用云计算服务的主要原因之一。对于用户来说，他们不希望重要数据被其他任何无关公司尤其是竞争对手获得。云计算服务提供商也应该恪守信息不扩散守则并且为任何信息泄露事件负责，就像银行有义务保护所有储户的个人信息一样。

2. 法律法规

作为一个新兴产业，云计算产业尚缺乏法律、法规去规范云服务提供商和用户的行为准则。这些准则需包括规范云计算服务提供商服务连续性、安全性、私密性等方面的责任；用户滥用、恶意使用云计算应用的定义和合理使用规范。用户也可以通过分析对这些法律法规的遵从程度来判断和选择云计算服务提供商。

3. 使用监控

云计算系统需要能够判断用户的非恰当使用、滥用和恶意使用云计算服务的场景，阻止这些现象的发生，并且识别出这些用户。例如，阻止用户使用云计算系统发起洪水攻击，发送垃圾邮件，非法暴力破解密码。

4. 耗能监控

传统的企业 IT 系统每年的耗能是巨大的，据统计每个设备三年消耗的电价与设备购买的价格基本等同，所以云计算系统的耗能管理是非常重要的一个问题。由于虚拟机是云计算系统的基本组成单元，而每个硬件设备上往往设置有多个虚拟机，所以云计算提供商需要合理地划分和管理虚拟机以求开启的硬件设备最少从而达到节能的目标。

5. 基于云的反病毒、反垃圾邮件

基于云计算架构的反病毒和反垃圾邮件的研究也在渐渐兴起。基于云计算的反病毒须将威胁模型数据库和分析引擎都植入云计算平台中，云计算强大的计算能力和实时交互能力对共享流量模型和威胁分析结果有非常大的帮助；基于云计算的反垃圾邮件可以通过云计算平台将每个邮件都打上签名标记来判断某一邮件是否是另一邮件的拷贝。目前这一领域尚不成熟，如何有效地共享攻击模型、准确判断威胁、建立合理的商业模式等问题尚待解决。

6. 在云系统中构架可信计算

目前企业用户对将其重要数据迁移到云计算系统的最大忧虑在于缺乏对云计算供应商的信任。从根源上说，可信计算平台是一个以可信根为基础的通用安全体系结构，赋予所有在计算平台上执行的代码一个未被篡改环境，包括基于应用程序层面、操作系统层面和硬件层面可信环境。在云计算系统中构架可信计算的第一步则是对可信根的定义。RSA 建议将云计算系统中所有计算单元都植入可信计算芯片作为可信根，并以此为基础构架可信计算系统。遗憾的是这种方案的可操作性较差，成本也较高。

类比电力网络的发展史，基于传统的计算方式的企业 IT 系统就好像一台又一台的发电机。这些发电机以个体和集群的方式出现在各个企业中，为了防止单点故障，企业往往需要投资建造备份的发电设备。而基于云计算方式的企业 IT 系统就好比是淘汰了发电机转而使用集中发电、电网输电的用电方式，用电成本被大幅降低，电力的稳定性和安全性也大幅提高。所以，就像集中发电代替个体发电的历史一样，云计算服务替代现有的企业 IT 系统是无法回避的发展趋势。

云计算作为下一代计算模式全面进入实践阶段。标准和互操作问题成为云计算发展的瓶颈，众多标准组织都把云的互操作、业务迁移和安全列为云计算三个最重要的标准化方向。云安全被认为是决定云计算能否生存下去的关键问题，开展云计算安全标准的研究，制定云安全相关标准，已成为亟需解决的问题。目前大多数国家都是以政府为主导在逐步推动云计算，比如美国发布的云优先战略、英国的政府云、日本的霞关计划等。美国尤其指定了 NIST 为云计算研究制定相关标准。我国政府也先后出台了多项政策推动云计算，因此，云计算安全标准应首先对云计算安全问题进行深入分析，尤其是数据保护方面，抓紧对数据隔离与管理、身份管理等关键技术的研究，梳理和比对已有安全标准，逐步制定云计算安全技术保障标准和关键技术标准。

同时，政府部门应从云计算安全监管的角度进行研究，规范政府部门云计算应用的安全管理及技术要求，以保证政务云的安全稳定运行。建立对云服务提供商的安全测评指标体系，对云服务提供商的资质、安全服务能力和服务质量以及如何对云安全服务进行检测进行规范。

此外，标准是引导和规范云计算产业健康持续发展的因素之一，而国家相关法律法规的制定，如数据保护法、个人信息保护等则是相关标准实施的基础，本书也呼吁国家尽快制定相关法律法规，切实保护公民个人利益，并推动云计算等技术新应用的发展和繁荣。

第6章 企业信息安全框架

传统信息安全建设方法大都从“单个系统”出发，很少考虑整个组织的全局信息安全，因为复杂大系统的分解和差异性安全要求描述很困难。但实际工作应该是从组织整体出发，整体考虑所有系统。如果各系统单独保护，将对组织产生冲突和割裂，形成信息孤岛；各系统安全单独建设，将造成分散、重复和低水平。目前的信息安全在建立长效机制方面考虑较少，难以做到可持续运行、发展和完善。

因此，我们应从组织整体出发，综合考核所有系统，引入安全体系设计方法，引入保护对象框架设计方法，引入安全平台的设计与建设方法，准确地进行大系统的分解和描述，反映实际特性和差异性安全要求，这样，我们就导入了企业信息安全框架的概念。本章首先描述了信息安全框架的概念，其次论述了企业信息安全框架的基本组成和内容以及其相互的关联，最后给出了企业建设信息安全框架的目的意义。

6.1 信息安全框架概述

本节我们根据企业信息安全实际情况导入一个信息安全框架的概念，明确企业信息安全框架的定义，并进一步论述企业信息安全框架的要素组成与具体内容。

6.1.1 信息安全框架的引入

企业信息安全是以建立企业信息化空间可信环境与秩序作为发展目标的，不仅要保障数据与系统的安全，还要对基于参与者主体的“行为与内容”进行资源管理、认证及监控。因此，企业信息安全的重要任务是通过把企业内外部相互孤立的信息安全资源集中、整合起来，在一个安全框架内构成专门的管理、监管、认证和控制功能或职能，形成一个信息安全体系。使企业信息安全从关注产品、系统脆弱性的局部安全逐步发展到基于企业战略、业务为主线来关注信息安全组成与结构的整体安全。企业信息安全需要从全方位的视角去管

理，而不是通过单一系统或程序来实现。企业战略、安全标准、作业流程、安全组织，规范制度，甚至安全工具与实施手段等都是环环相扣的，都是企业实现信息安全建设目标的必要因素。

随着信息化社会进程加速，企业处于一个越来越复杂的信息环境中，使用传统的系统方法开发信息安全解决方案时往往会遇到很多挑战。例如，系统安全平台需求开发的困难性；云计算应用对企业传统安全的挑战；多平台、多组件架构的安全功能平台整合的复杂性，以及安全解决方案实施的多样性。这些都会使企业在实际的安全实践中陷入困境。所有企业信息化过程中面临着普遍的信息化安全问题，企业的安全自主保障体系建设、企业信息化的监管体系建设、企业的安全应急与业务连续性建设都存在或多或少的问题。

通过分析企业信息安全构成要素，我们可以进一步为企业构建一个信息安全框架以提供实际指导意义。企业通过一个完整的信息安全框架，可以促进企业能够根据自身的实际情况判断信息安全建设水平并发现其中的问题。企业信息安全要素分析与框架指南，可以帮助不同规模、处于不同信息化实施阶段的企业明确进一步信息安全建设的各个层面和各个环节应该达到的目标和努力的方向。企业信息安全框架将信息安全工作中的各种要素加以提炼，形成可以量化的核心要素，为企业提供广泛的指导性建议，也为安全厂商的产品开发、深刻理解企业信息安全提供帮助。

6.1.2　信息安全框架研究与定义

企业管理者渴望获得有效的手段来管理和控制企业的各种风险，他们需要了解安全风险对信息系统以及相关业务所产生的潜在影响，并且需要获得应对这些风险的快速有效的措施来保障相关业务的可用性和稳定性。与此同时，他们还需要通过加强合规管理、业务流程优化来提高企业安全风险管控。由此可见，企业信息安全系统中的各个安全组件或要素只有整合成为一个整体协同作用时，才能有效保证企业整体安全管控的目标得以实现。然而，对于大多数企业或组织来说，在信息安全建设过程中，并没有形成一个清晰的安全框架来确保企业的风险管控。因此，如何根据企业业务发展的需要，明确合理的信息安全需求，确立企业信息安全框架，选择安全功能组件将对企业管理者和企业 IT 人甚至相关安全厂商是一个挑战。

企业信息安全框架可以帮助我们全面理解和解决企业 IT 基础架构中与安全有关的各种问题。通过这个全面的，基于安全最佳实践和业界相关开放标准的安全模型，可以帮助企业定位安全建设的现状、了解安全建设的需求、组织未来安全建设的规划和实施。它为企业提供了一个自上而下的、整体的信息安全建设视图。

企业信息安全框架就是企业以信息安全目标为导向，依据信息安全最佳实践和标准，明确企业中信息安全各个过程和环节，确定信息安全建设基本的内

容，如图 6-1 所示的企业整体的信息安全建设视图。

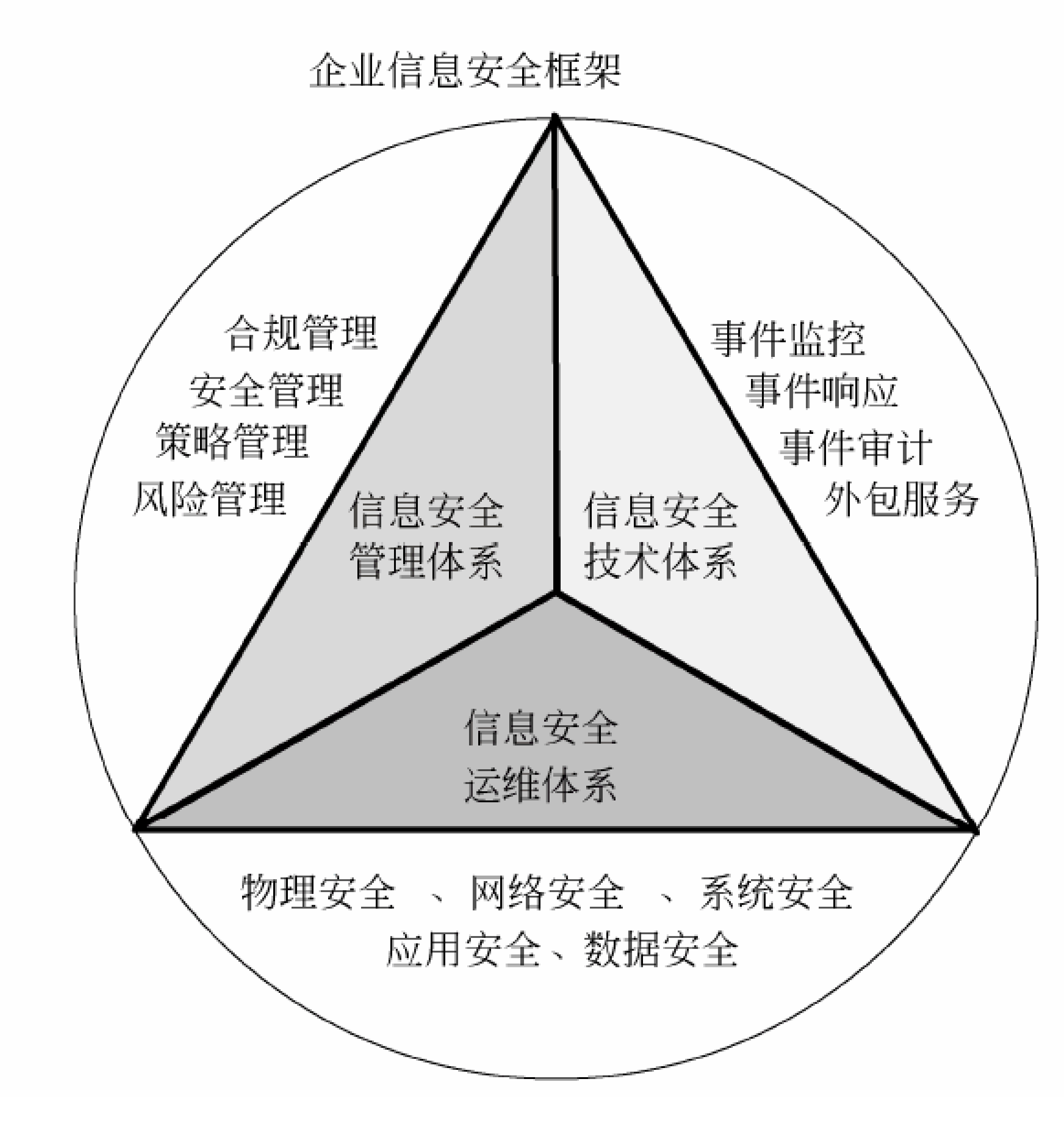


图 6.1 企业信息安全框架

6.1.3 信息安全框架要素与组成

企业信息安全框架要考虑企业的多样性。企业类型的多样性决定了它们信息安全建设的重点和关注也有所不同。企业根据生产方式不同至少可以分为三大类型，即制造型企业、流通型企业、服务型企业。以制造型企业为例，企业信息化以生产制造业务为核心，信息安全的主要关注点是生产流程可靠性与设计生产一致性。另一方面，对信息安全服务提供商来说，由于企业在生产及管理流程上存在很大差异，用一套框架或系统服务于所有行业、不同规模的企业，无论从管理学还是方法学的角度都是不现实的。因此，正确对待行业差异性，是企业信息安全框架不可避免的问题。我们综合分析国内企业信息安全建设经验，总结各个行业信息安全框架的核心要素，结合国际、国内相关标准与最佳实践，提出企业信息安全框架中的各个核心要素及其结构。

企业信息安全是一项系统性、改造性工程，企业信息安全框架涵盖了信息安全过程中各个方面和各个环节，既有战略层次要素，也有管理层次、操作层次要素；既有衡量性能的要素，又有衡量技术、管理的要素；既有外部环境要素，又有内部因素；既有较为抽象的一级要素，又有非常具体的二级、三级要素。可以说，企业信息安全框架是立体交叉的体系结构，能为企业信息安全提供全面的指导。其中，一级要素为分类要素，二级要素为过程或流程要素，三级要素为指标要素。要素关系如图 6-2 所示。

6.1.4　信息安全框架内容简述

企业信息安全框架中的要素分析，其中一级分类要素很关键，有些框架完全按照信息安全技术过程分类，这种信息安全框架不是企业的，是信息安全产品提供商或服务商的，企业按照这样的框架作为指导，只能是大量的采购产品；有些框架按照管理对象分类，把资源、管理、人员、技术等分离开来，则必然造成了企业信息安全运行效率低下的问题。这样，企业信息安全框架的分类要素对于企业管理者至关重要，但提出合理的、高效的企业信息安全框架却比较困难。

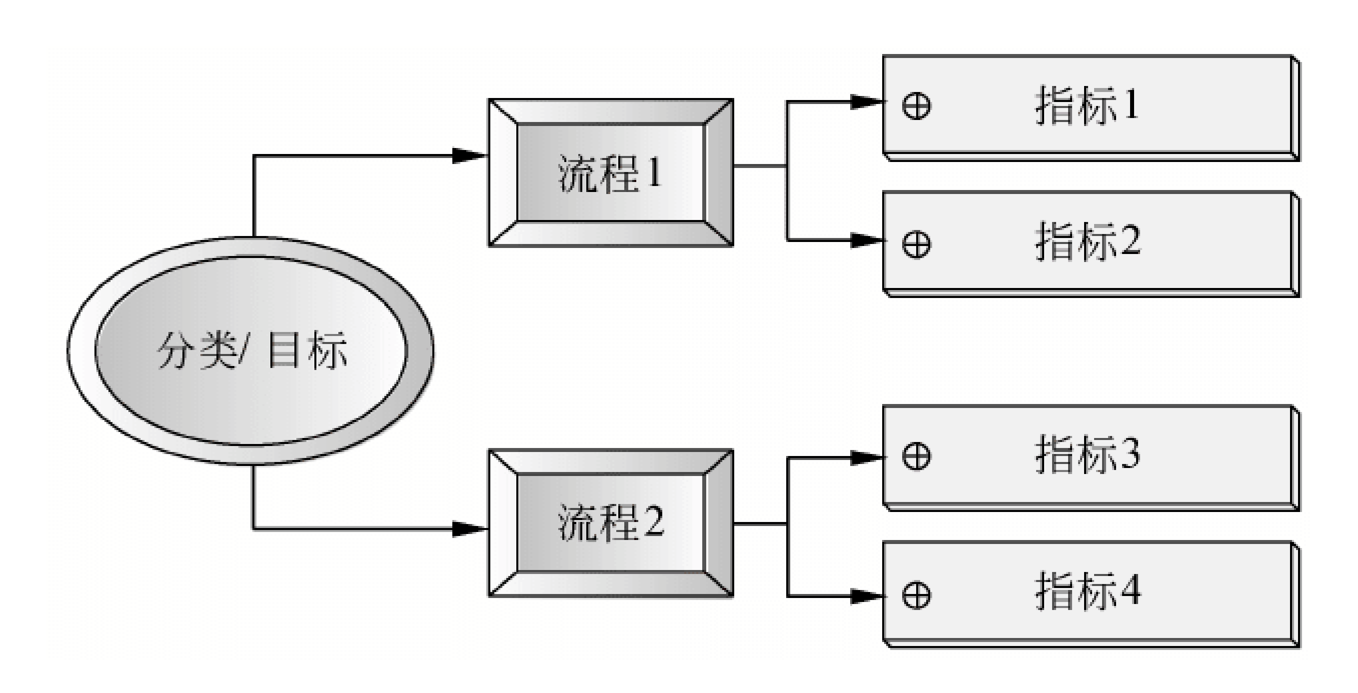


图 6-2　企业信息安全框架要素关系说明

我们知道，信息安全框架最终的核心任务是完成或达成企业信息安全目标，企业信息安全目标同样是一个企业信息化的目标之一。那么，企业信息安全框架应该和企业信息化的体系结构设计一脉相承；同时，企业信息安全框架是企业各级人员对企业信息安全的视角与关注，并需要通过视图或模型来描述，如图 6-3 所示。

在 IEEE 1471 中，对体系结构有如下解释：一个领域有多个系统，系统受到环境的约束。系统有一个体系结构和多个关注者。每一个关注者对系统都有多个关注，有自己的多个视点，并对体系结构描述（AD）识别。体系结构被体系结构描述说明，在说明中要阐述理由。关注要对体系结构描述识别，要被视点所覆盖。视点划分或选择体系结构，并被视图所体现或得到遵守，并建立模型。视图由模型所组成，体系结构描述由视图和模型所汇聚。

运营体系结构是实现或支持业务运营的任务、活动、运营元素和信息流的描述，定义了信息交换的类型和模式，定义了信息交换支持的任务与活动，定义了如何支持信息交换的互操作性。运营体系结构包括以下内容：

（1）运营体系结构的基本目标是定义运营元素、活动与任务和信息交换需求及模式。

（2）描述多业务的关系和多业务结构。

（3）描述业务与活动的指标体系。

（4）业务与活动是跨越组织边界。

（5）运营体系结构通常没有系统依赖性，是和组织体系结构相关的。

（6）运营体系结构定义是一个设计过程，关注点不同，其描述的内容也不同。

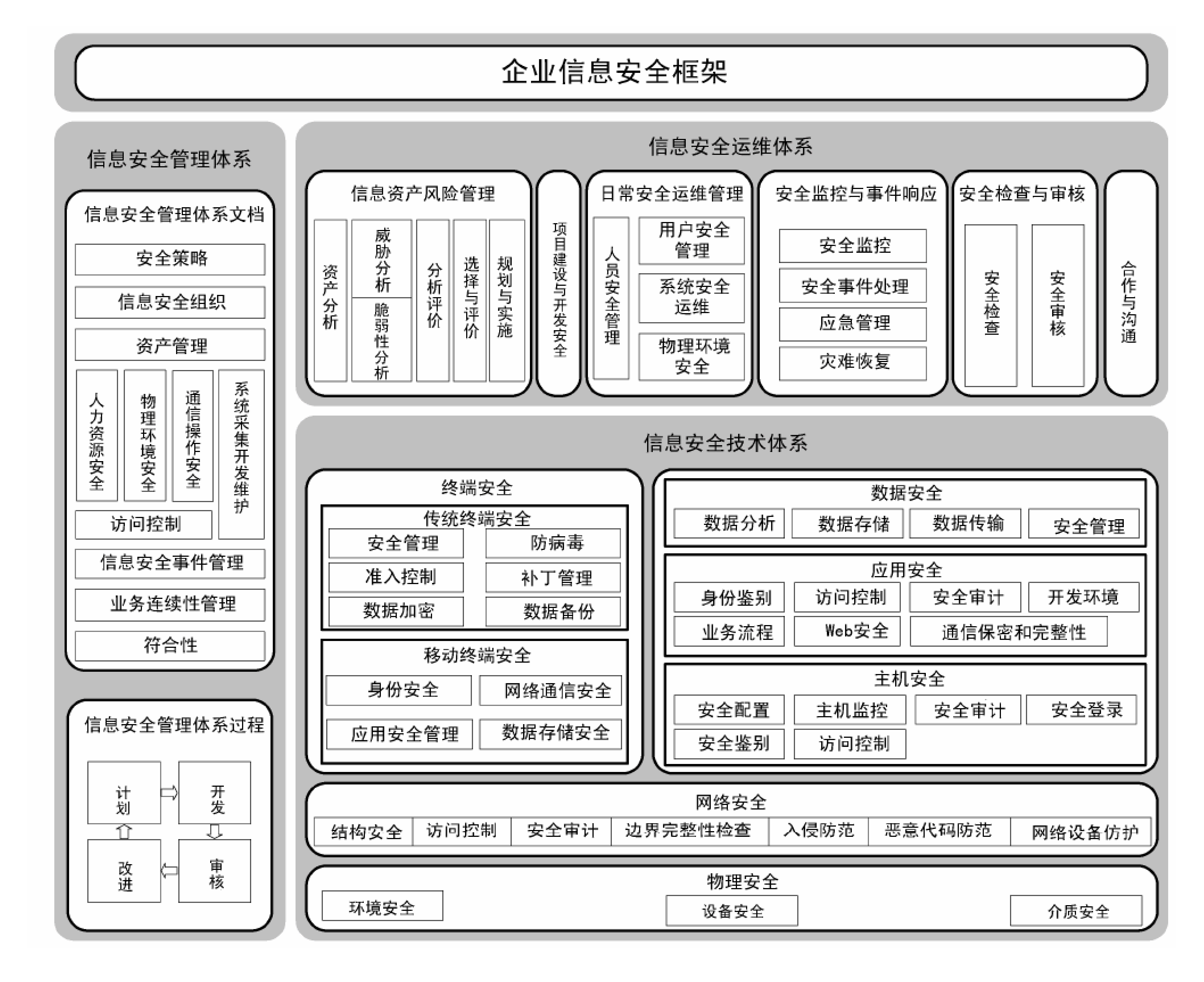


图 6-3　企业信息安全框架

系统体系结构是提供或支持业务功能的系统或系统之间连接和互操作的描述。系统体系结构包括以下内容原则：

（1）系统体系结构的基本目标是描述系统的应用，实现运营任务和活动的完成。

（2）系统体系结构描述系统的内部结构，描述系统关注的技术与功能特性的实现要求。

（3）系统体系结构描述面向多业务的多系统体系结构，描述如何实现多个系统连接和互操作的，标识系统接口和定义系统之间的连接性，定义了系统行为的约束和范围。

（4）描述系统在业务与技术组织机构中的分布。

（5）系统体系结构可以支持多组织与领域。

（6）系统体系结构用其发展的时间阶段来标识。

（7）系统体系结构是基于技术体系结构的，并且被技术体系结构所约束。

（8）系统体系结构定义是一个设计过程，关注点不同，其描述的内容也不同。

技术体系结构是系统的最小规则的集合，这些规则控制着系统元素或部件的配置、交互和相互间的依赖性，其目的在于确认系统满足一定的标准、规范、规则、准则和要求所组成的框架。技术体系结构包括以下内容：

（1）技术体系结构是基于运营需求和所支持系统之间的协调的，为系统选择合适的技术和互操作性准则。

（2）技术体系结构基本目标是定义一个标准的和规则的结合，用这些标准与规则来控制系统实现、运营、管理和维护等任务。

（3）技术体系结构标准和准则应当反映多信息系统实现环节。

（4）技术体系结构说明了在所有系统中是多平台和网络互联的要求。

（5）技术体系结构必须提供融入新技术和技术演化的标准和老技术逐步退出的策略。

（6）技术体系结构应当是逐步走向采用商用标准，并向这个方向发展。

依据信息化体系框架的标准，企业信息安全框架一级要素如图 6-4 所示。



图 6-4　企业信息安全框架一级要素视图

一级要素分别为：安全管理、安全运维、技术体系。

安全管理：主要包括信息安全建设的战略和治理框架、风险管理框架以及合规和策略遵从。安全治理、风险管理和合规是企业信息安全框架的最顶层，是企业业务驱动安全的出发点。通过对企业业务和运营风险的评估，确定战略和管理框架、风险管理框架，定义合规和遵从，确定信息安全文档管理体系。

安全运维：是指在安全策略的指导下，安全组织利用安全技术来达成安全保护目标的过程。安全运维与 IT 运维相辅相成、互为依托，共享信息与资源。

安全运维与安全组织联系紧密，融合在业务管理和 IT 管理体系中。安全运维包含威胁分析与预警，安全状态和事件的监控，安全事件或事故的响应，以及基于安全目标的操作行为和日志审计，这些安全运维的任务主要可通过安全事件监控、响应、审计和相应的安全策略体系共同完成。

技术体系：是指物理安全、基础架构安全、身份/访问安全、数据安全和应用安全。技术体系是安全运维和管理的对象，其功能由各自的子系统提供保证。

6.2 信息安全框架基本内容

企业信息安全建设围绕企业信息安全框架的基本要素，分为安全管理、安全运维、安全技术建设三个层面，并且在各个层面自成体系，依据框架不同视图之间的关系，相辅相成。本节分别阐述企业信息安全框架中的二级、三级要素视图。

6.2.1 安全管理

企业信息安全管理体系框架是企业信息安全框架中的业务视图，是企业信息安全目标的分解视图，依据 ISO 27001 的信息安全管理体系要求，采用“计划、实施、检查、改进”过程模式建立企业的信息安全管理体系，如图 6-5 所示。

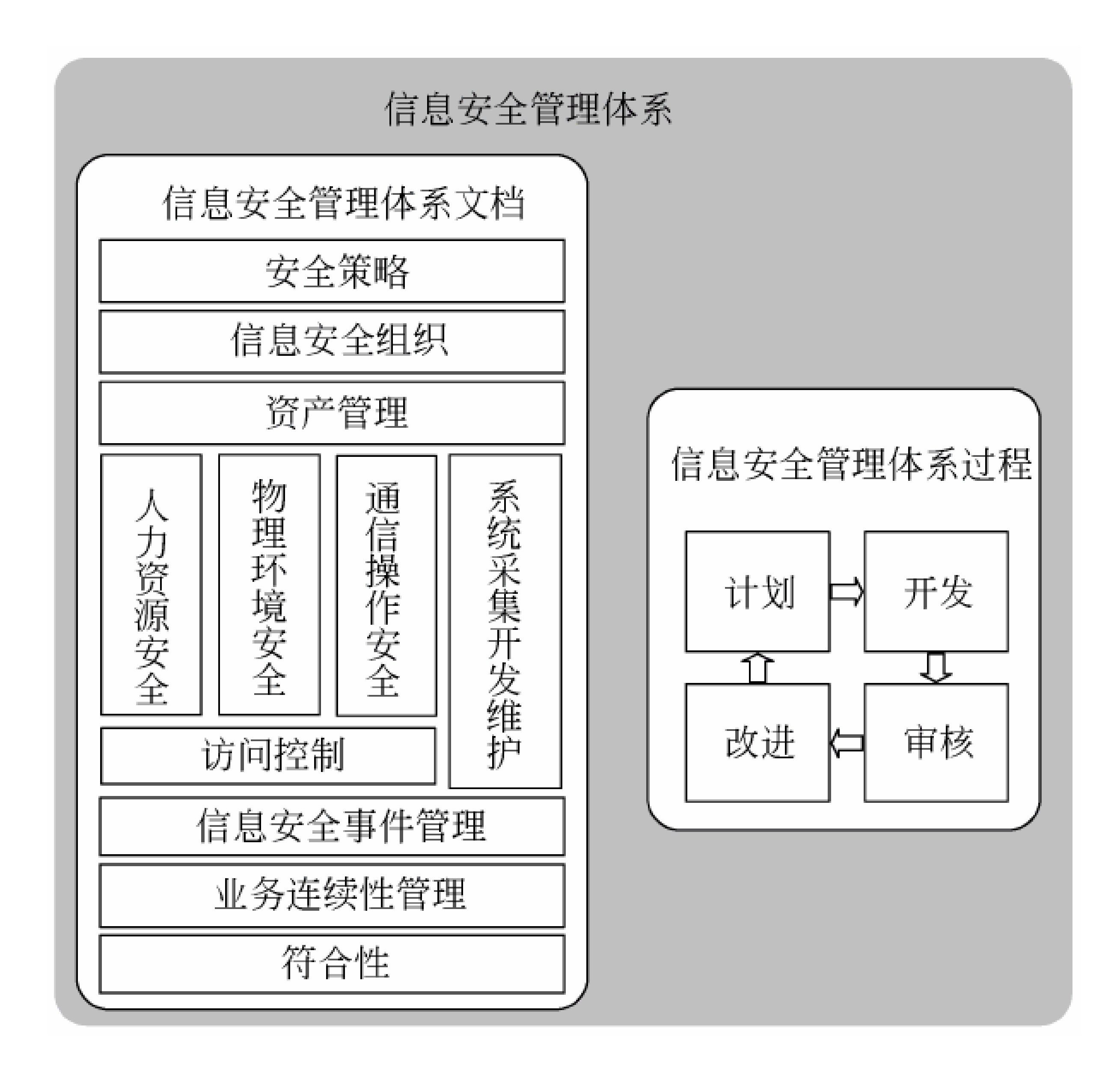


图 6-5 信息安全管理体系

（1）计划：依照企业整个方针和目标，建立与控制风险、提高信息安全有关的安全方针、目标、指标、过程和程序。

（2）实施：实施和运作方针（过程和程序）。

（3）检查：依据方针、目标和实际经验测量，评估过程业绩，并向决策者报告结果。

（4）改进：采取纠正和预防措施进一步提高过程业绩。

以上四个步骤成为一个闭环，通过这个环的不断运转，使信息安全管理体系得到持续改进，使信息安全绩效螺旋上升。对应策略、实施、检查、改进四个环节，企业信息安全管理视图可包括以下流程：合规管理、信息安全管理、信息安全策略管理、风险评估管理。其中，合规管理是企业信息安全管理体系的基石，信息安全治理与策略管理是企业信息安全管理体系的主体梁架或骨架，风险评估管理是企业信息安全管理体系建设的重要内容，如图 6-6 所示。

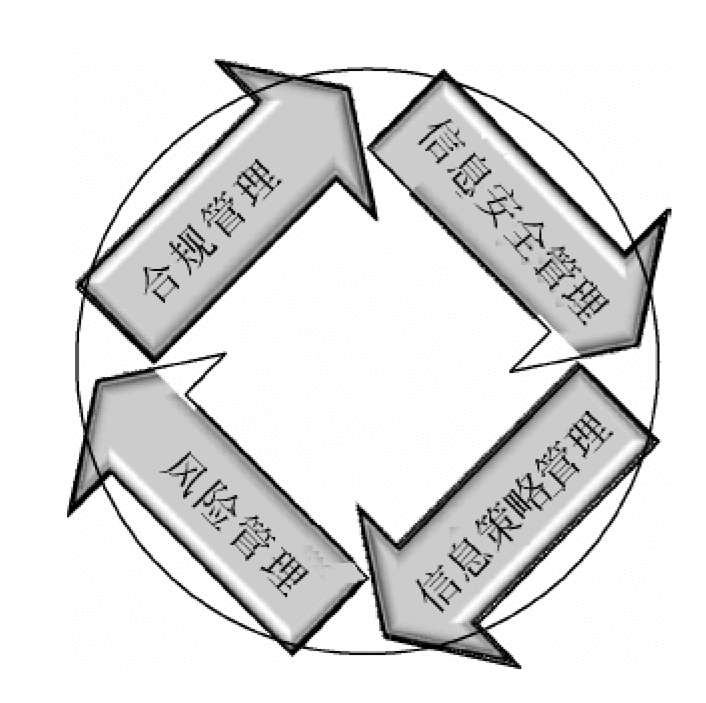


图 6-6　企业信息安全管理视图

合规管理：对外部监管机构、法律法规相关要求定期跟踪、收集的流程，为满足监管要求对企业制度的分析与更新流程。其包括合规采集、合规审计等指标。

信息安全管理：针对企业整体信息化和信息安全战略目标及业务目标，对组织、结构、人员、制度、考核等相关规划、设计与贯彻的过程。其包括规划管理、制度管理、资源管理、人员管理、监督管理、违规管理、外部管理等指标。

信息安全策略管理：企业信息安全业务的整体规划和落实计划的建立、更新与废弃等流程，包括规划、方案设计、落实等指标。

风险管理：企业对由于管理流程及资源缺失或不足、自然因素、人为因素和技术漏洞产生的操作、法律、声誉等风险的识别、评价、处置等流程，包括风险识别、风险评估及评价、风险处置、整改等指标。

6.2.2　安全运维

企业信息安全运维体系在企业信息安全框架中是信息安全的系统功能视图，是企业信息安全业务目标与信息化各个环节相关联后，企业信息安全目标的系统化分解、系统化运行的核心视图。

在安全策略的指导下，安全组织利用安全技术来达成安全保护目标的过程。安全运维与 IT 运维相辅相成、互为依托，共享信息资源。企业安全运维主要包括安全监控、事件响应、事件审计、外包服务等流程，如图 6-7 所示。

安全监控：重要功能需求主要包括安全事件的收集、安全事件的归并和过滤、安全事件标准化、安全事件显示和报表。

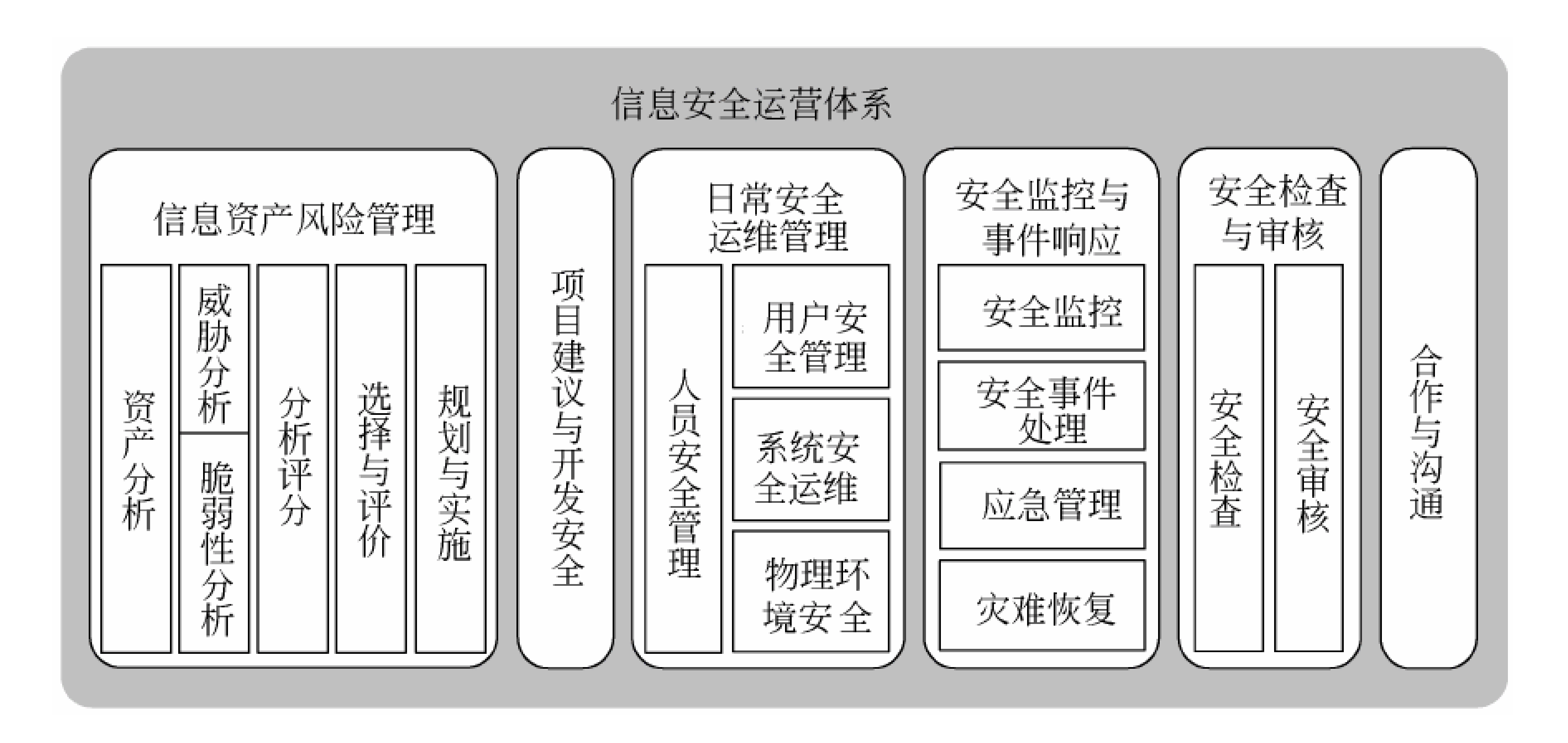


图 6-7 企业安全运维视图

事件响应：需要企业安全人员提供工具、工作流以及报告，可减少攻击识别和补救之间的时间，风险处置流程分为自动响应和工单管理两大部分。

事件审计：对用户操作行为、维护行为记录的分析与处理过程。不建议将安全审计外包。

外包服务：安全外包是将自身的安全运维工作外包给外部专业的安全管理服务商，依赖外部的专业力量来协助组织自身的安全运维工作，实现安全托管。

技术体系更多是解决安全风险点的问题，也就是我们常说的“就事论事”：有病毒杀病毒、有漏洞补漏洞等等。但是我们知道，信息分散在一系列工作流程的各个环节中，因此需要对各项日常运行工作流程进行安全控制，也就是从信息的生命周期进行流程控制，即在信息的创建、使用、存储、传递、更改、销毁等各个阶段进行安全控制。在运维体系建设中，往往需要结合ITIL、COBIT 等流程分析来关注信息的生命周期安全。

6.2.3 安全技术

企业信息安全技术体系是企业信息安全的技术视图，是企业信息安全业务目标与信息化各个环节关联后，在信息安全技术方面的技术指标分解。它主要包括物理安全、基础架构安全、身份/访问安全、数据安全和应用安全的技术机制和技术管理等流程。技术是安全必不可少的实施工具，采取哪些安全技术，市场上有哪些工具可以使用，这是绝大部分信息安全管理工作者最关心的话题。一般来说，可以按照从上到下信息所流经的设备来部署工具，即从数据安全、终端安全、应用安全、主机安全、网络安全、物理安全六个方面来选择不同的安全工具。信息安全工具种类繁多，一般而言，每一种工具都有其擅长的安全方面，因此应按照“适度防御”原则，综合采用各种安全工具进行组合，形成企业“适用的”安全技术防线。最后，需要一到两种提供综合管理的工具来帮助把所有的安全监控工具进行统一管控。这个和最终希望呈现给使用者的目的有所不同。例如，SOC（安全运行中心）是给企业日常维护管理者使

用的；ITRM（风险管理工具）作为综合风险呈现，是给企业风险或安全管理层使用的。信息安全技术体系如图 6-8 所示。

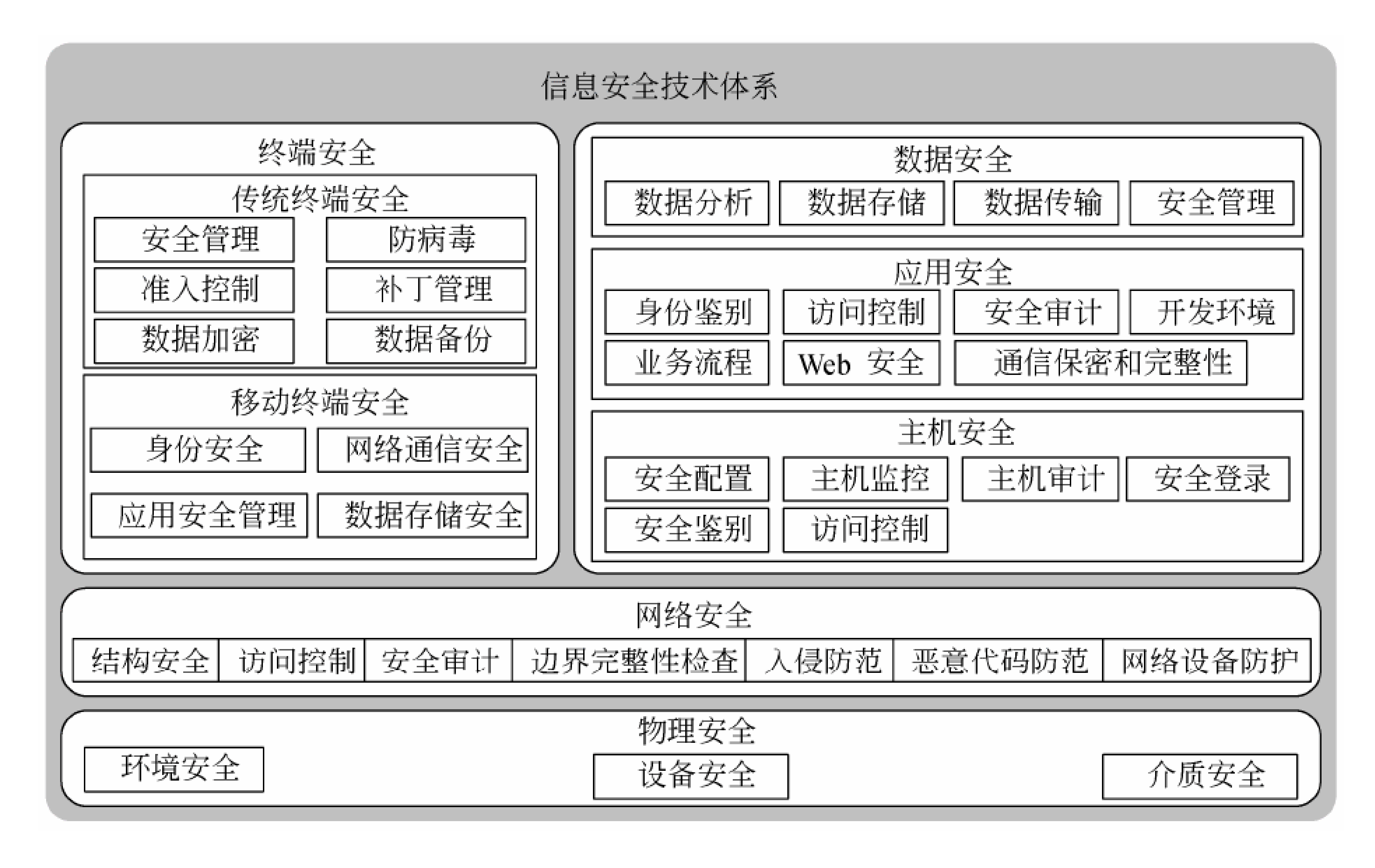


图 6-8　信息安全技术体系

6.3　信息安全框架建设的意义

企业信息安全框架建设的意义旨在给企业信息安全建设提供一个集成的、标准的企业信息安全框架，帮助企业快速知晓企业信息安全的现状和需求，为企业信息安全平台的建设、设计、实施提供指导和参照。它包括以下内容：

（1）帮助企业了解企业信息安全建设的整体状况；

（2）帮助企业找出现有安全系统可能存在的差距；

（3）帮助企业识别业务风险，系统了解风险状况；

（4）帮助企业在安全建设中合理定义安全需求和建设的方向；

（5）全面分析、评估企业信息安全政策、标准和指南及其日常执行情况，衡量其是否能够有效地保障公司的信息安全；

（6）帮助企业制定核心信息安全管理流程，初步建立有效的信息安全体系；

（7）完善企业的信息安全架构蓝图及路线图。

第7章

信息安全管理体系

大多数企业的信息安全管理工作在企业信息安全建设中明显滞后于信息安全技术工程项目建设。企业信息安全管理经历了从操作规范管理到业务流程管理，最后到管理体系建设这样三个阶段。在企业信息安全框架的研究与建立中，我们将企业信息安全管理的体系建设作为企业信息安全建设的首要任务。

企业信息安全管理体系建设是企业信息安全框架中的业务视图，是企业信息安全工作的启动、建设、规划的重要内容，如果没有企业信息安全管理体系的建设就没有企业信息安全。本章基于第 6 章所描述的企业信息安全框架中的信息安全管理视图基础上，进一步从企业信息安全合规管理、信息安全管理、信息安全策略遵从以及信息安全风险管理四个层次来阐述如何构建企业信息安全管理体系。

7.1 信息安全合规管理

企业信息安全合规管理是企业信息安全管理体系建设的启动、规划，或者是任何其他管理环节都必须要考虑的基本要素。它是企业信息安全管理体系建设的基石和助推器。

7.1.1 信息安全合规管理挑战

2005 年，巴塞尔银行监管委员会发布了《合规与银行内部合规》监管准则，同年，美国证券业协会发布《合规的作用》。2006 年，国际证监会组织技术委员会发布《市场中介组织合规职责问题的最终报告》。2008 年 7 月 14 日，中国证监会发布《证券公司合规管理试行规定》，标志着合规管理成为中国证券公司日常经营管理的一项常规工作。同样，其他行业在不同的时期，都对国家相关标准、法律法规、行业规范等进行采纳，并吸收成为本企业信息安全管理基本指导方针的必要和需要。

从公司管理的角度看，合规经营是企业管理层履行受托责任的基本要求，也是防范企业管理层道德风险的制度保证。

从企业的社会责任角度看，企业面向的客户、市场，安全稳健运行是其经营的生命线，因此，合规经营是企业履行社会责任的具体体现。

7.1.2 信息安全合规管理概述

合规就是必须符合法律、法规和准则。企业合规管理不追求经营活动的变通和弹性，它更强调“立规矩，定方圆”。合规管理是企业管理的立身之本，也是现代企业管理的重要内容，更是监管部门的常规监管要求。企业信息安全合规管理与企业信息安全管理和全面风险管理是企业可持续发展的三种制度安排和保障。同时，在合规与业务发展发生矛盾时，合规优先于业务发展必须是企业经营的基本方针。企业信息安全合规管理需要处理好以下三类关系：

1. 合规管理与内控

企业信息安全管理与策略管理可以统称为企业信息安全管理的内控，信息安全合规管理是内控的基石，内控是合规的环境。例如，2008 年 6 月，财政部、证监会、银监会、保监会及审计署五部委联合发布了“中国版萨班斯法案”——《企业内部控制基本规范》，并于 2009 年起首先在上市企业中实施。该规范中明确内部控制的目标，即战略目标、经营目标、报告目标、合规目标。内部控制涵盖企业的整个经营活动，保证企业合规经营，防止舞弊的环境和进行程序保障。

2. 合规与业务发展

在企业的经营管理中，合规经营与追求经济效益同等重要，不能把合规管理视为业务发展的障碍。在合规与业务发展发生矛盾时，必须坚持合规优先。企业不论是在制定业务操作和管理规章制度时，还是在开发新产品、新业务，以及营销市场、服务客户时，都必须要首先按照内部控制的流程对其评估，测量合规风险。

3. 合规与全面风险管理

合规管理是企业全面风险管理的重要组成部分。从风险管理的角度看，合规能够帮助企业规避各种风险，避免触犯法律法规，降低因遭受监管处罚和法律诉讼而导致财务损失的可能性。

7.1.3 信息安全合规管理工作

企业信息安全合规管理工作可以包括以下内容：

1. 监管要求采集

监管要求采集中的关键活动包括监管要求跟踪和监管要求汇总。从关键活动的缺失和有效性来看监管要求采集的风险，包括监管要求梳理机制、监管要求的跟踪、对监管要求进行汇总，并对形成规范的监管要求列表。

2. 监管合规管理

监管合规管理中的关键活动包括监管要求差距评估和差距评估结果的整改落实。从关键活动的缺失和有效性来看监管合规管理的风险，包括以下方面：

（1）依据监管要求，对 IT 管理现况的差距评估；

（2）根据差距评估结果形成规范的 IT 管理变更需求。

7.2 信息安全管理

企业信息安全管理是在企业信息安全合规管理的基础上，企业将外部法律、法规、业务需求、技术环境融合成为企业自身信息安全的行为规范、标准、手册、制度、文化等的过程。

7.2.1 信息安全管理挑战

企业信息安全管理首先要明确企业的哪些资产需要保护：企业必须花费时间与精力来首先确定关键数据和相关的业务支持技术资产的价值。通常，各公司认为表述资产的价值是很容易的，但具体如要按级别界定就不那么简单了。其次，还需完成威胁识别及风险评估的任务：如果企业想增强竞争实力，必须随时改进和更新系统和网络，但是机会增加常伴随着安全风险的增加，尤其是机构的数据对更多用户开放的时候，因为技术越先进，安全管理就越复杂。

信息安全管理问题之所以成为企业管理中很难解决的一个问题，主要原因在于：信息资产与物理资产的差异性。一般而言，信息资产与物理资产的基本区别是，信息资产是动态变化的，而物理资产是固定不变的。信息资产在许多方面表现出动态特征——从信息以运行数据（客户账户、业务交易等）的形式产生开始，直到在各种业务功能和过程中最终的应用（ERP、CRM、商业智能）。IT 界为信息生命周期的每一个阶段推出了许多单一性的产品。这些产品分别用于解决生命周期中某个方面的问题，包括信息的生成、处理、分布、存档、检索和处置。某一种信息资产在生命周期的每一个阶段各有其价值，而且，一般来说它的价值会随着生命周期的进展而增加。因此，企业的这种动态资产在其进展的每一步中必须受到保护，以防止外部和内部的威胁。遗憾的是，技术厂商们至今并不能出色地提供这些产品功能以保护信息安全。

由于 IT 是管理企业不可或缺的工具，企业管理层如何履行他们的基本职责以保护公司最有价值并且是动态的资产：公司信息的整体？当然，对于常见和已知的安全薄弱环节，现在和将来会不断出现新的产品，如防病毒、防火墙以及加密等。正如我们已经论述的，技术手段是必要的，但不足以解决信息资产保护的全部问题。完整地看，还有其他方面要考虑：与技术结合在一起。信息安全管理的核心是一种管理业务风险的机制，而不仅仅是技术风险，它是一种能够使业务运转和增长的方法。与业务需求相对应是实施信息安全程序的关键，并使其对企业具有实际意义。

当前企业在信息安全管理中普遍面临的问题：

（1）缺乏来自法律规范的推动力和约束；

（2）安全管理缺乏系统管理的思想，被动应付多于主动防御，没有做前期的预防，而是出现问题才去想补救的办法，不是建立在风险评估基础上的动态的持续改进的管理方法；

（3）重视安全技术，忽视安全管理，企业愿意在防火墙等安全技术上投资，而相应的管理水平、手段没有体现，包括管理的技术和流程，以及员工的管理；

（4）在安全管理中不够重视人的因素；

（5）缺乏懂得管理的信息安全技术人员；

（6）企业安全意识不强，员工接受的教育和培训不够。

7.2.2　信息安全管理概述

企业信息安全管理即针对当前企业面临的病毒泛滥、黑客入侵、恶意软件、信息失控等复杂的应用环境制定相应的防御措施，保护企业信息和企业信息系统不被未经授权的访问、使用、泄露、中断、修改和破坏，为企业信息和企业信息系统提供保密性、完整性、真实性、可用性及不可否认性服务。简而言之，使非法者看不了、改不了信息，系统瘫不了、信息假不了、行为赖不了。这样的防护措施是从企业角度的、全方位的防护，它涵盖了制度、人员机构、技术、资源等诸多方面。与企业其他管理，比如质量管理一样，是标准化、系统化的建设。

7.2.3　信息安全管理工作

企业信息安全管理工作内容如下：

1. 制定安全方针

安全方针是关于在企业内指导如何对信息资产进行管理、保护和分配的规则、指示，是企业信息安全管理体系的基本法则。企业的信息安全方针，描述信息安全在企业内的重要性，表明管理层的承诺，提出组织管理信息安全的方

法，为企业的信息安全管理提供方向和支持。

2．组织机构与职责分工

成立由企业主管领导任责任人的信息安全管理机构，管理机构具有以下职责：

（1）组织、协调和指导本企业信息化建设、使用和维护开发工作；
（2）组织制定信息化安全策略、流程和各种规章制度；
（3）组织信息安全风险评估及信息安全教育培训；
（4）组织信息化设备、设施、介质等授权使用和管理、维护、监督检查；
（5）落实年度安全计划、报告等；
（6）与国家相关主管部门建立日常工作关系；
（7）执行国家相关法律法规。

3．企业信息安全制度建立

企业信息安全管理机构组织建立相应的信息安全管理制度，明确岗位职责，实行领导责任制，层层落实，责任到人，使各个环节的每个工作人员明确应承担的职责和义务。信息安全管理制度要涵盖信息化的产生、存储、处理、传输、归档和销毁的全过程，从人员、物理设施与环境、设备与介质、运行与开发和数据安全等诸多方面制定相应的制度。

4．信息安全管理文件体系建立

（1）确立信息安全管理体系范围和体系环境所需的过程；
（2）战略性和组织化的信息安全管理环境；
（3）组织的信息安全风险管理方法；
（4）信息安全风险评价标准以及所要求的保证程度；
（5）信息资产识别的范围。

信息安全文件体系也可能在其他信息安全管理体系的控制范围内。在这种情况下，上下级控制的关系有下列两种可能：

下级信息安全管理体系不使用上级信息安全管理体系的控制：在这种情况下，上级信息安全管理体系的控制不影响下级信息安全管理活动。

下级信息安全管理体系使用上级信息安全管理体系的控制：在这种情况下，上级信息安全管理体系的控制可以被认为是下级信息安全管理体系策划活动的“外部控制”。尽管此类外部控制并不影响下级信息安全管理体系的实施、检查、措施活动，但是下级信息安全管理体系仍然有责任确认这些外部控制提供了充分的保护。

5．信息安全管理过程建立

（1）IT 规划管理：信息化规划制定和跟踪的流程。

（2）IT 制度管理：信息化管理制度体系化建设和完善的流程。

（3）IT 资源管理：对 IT 资源（包括人员、财务和 IT 资产）申请、审核、配备、评估的流程。

（4）监督管理：依据 IT 规划和制度对 IT 管理工作进行监督、检查和跟踪整改的流程。

（5）违规管理：对 IT 管理制度执行过程中的违规行为进行纠正与处罚的流程。

（6）外部环境：对影响 IT 管理目标实现的外部因素进行跟踪、响应、控制的流程。外部环境包括供应商管理、市场、经济环境、金融安全等。

6．信息安全管理条件与环境

（1）需要分配适当的资源（人员、时间和资金）运行信息安全管理体系以及所有的安全控制。这包括将所有已实施控制的文件化，以及信息安全管理体系文件的积极维护。

（2）提高信息安全意识的目的就是产生适当的风险和安全文化，保证意识和控制活动的同步，还必须安排针对信息安全意识的培训，并检查意识培训的效果，以确保其持续有效和实时性。

（3）如有必要对相关方实施有针对性的安全培训，以支持组织的意识程序，保证所有相关方能按照要求完成安全任务。

（4）还应该实施并保持策划了的探测和响应机制。

7．信息安全管理审核

（1）执行程序和其他控制以快速检测处理结果中的错误；快速识别安全体系中失败的和成功的破坏；能使管理者确认人工或自动执行的安全活动达到预期的结果；按照商业优先权确定解决安全破坏所要采取的措施；接受其他组织和组织自身的安全经验。

（2）常规评审信息安全管理体系的有效性；收集安全审核的结果、事故以及来自所有股东和其他相关方的建议和反馈，定期对信息安全管理体系有效性进行评审。

（3）评审剩余风险和可接受风险的等级；注意组织、技术、商业目标和过程的内部变化，以及已识别的威胁和社会风尚的外部变化，定期评审剩余风险和可接受风险等级的合理性。

（4）审核是执行管理程序，以确定规定的安全程序是否适当、是否符合标准以及是否按照预期的目的进行工作。审核的目的就是按照规定的周期（最多不超过一年）检查信息安全管理体系的所有方面是否行之有效。审核的依据包括 BS 7799-2：2002 标准和组织所发布的信息安全管理程序。应该进行充分的审核策划，以便审核任务能在审核期间内按部就班的展开。

8．管理者应该确保有证据

信息安全方针仍然是业务要求的正确反映；正在遵循文件化的程序（信息安全管理体系范围内），并且能够满足其期望的目标；有适当的技术控制（如防火墙、实物访问控制），被正确的配置，且行之有效； 剩余风险已被正确评估，并且是组织管理可以接受的； 前期审核和评审所认同的措施已经被实施；审核会包括对文件和记录的抽样检查，以及口头审核管理者和员工。 正式评审：为确保范围保持充分性，以及信息安全管理体系过程的持续改进得到识别和实施，组织应定期对信息安全管理体系进行正式的评审（最少一年评审一次），记录并报告能影响信息安全管理体系有效性或业绩的所有活动、事件。

9．改进信息安全管理

（1）测量信息安全管理体系满足安全方针和目标方面的业绩。
（2）识别信息安全管理体系的改进，并有效实施。
（3）采取适当的纠正和预防措施。
（4）沟通结果及活动，并与所有相关方磋商。
（5）必要时修订信息安全管理体系。
（6）确保修订达到预期的目标。

企业需要把措施放在信息安全管理体系持续改进的大背景下，以长远的眼光来打算，确保措施不仅致力于眼前的问题，还要杜绝类似事故再发生或者降低其再发生的可能性。企业的纠正措施的文件化程序有以下方面的要求：

（1）识别信息安全管理体系实施、运作过程中的不符合；
（2）确定不符合的原因；
（3）评价确保不符合不再发生的措施要求；
（4）确定并实施所需的纠正措施；
（5）记录所采取措施的结果；
（6）评审所采取措施的有效性。

企业应确定预防措施，以消除潜在不符合的原因，防止其发生。预防措施应与潜在问题的影响程度相适应。预防措施的文件化程序有以下方面的要求：

（1）识别潜在不符合及其原因；
（2）确定并实施所需的预防措施；
（3）记录所采取措施的结果；
（4）评审所采取的预防措施；
（5）识别已变化的风险，并确保对发生重大变化的风险予以关注。

7.3 信息安全策略管理

企业信息安全策略管理能保证企业信息化安全，保护工作的整体性、计划

性及规范性，以及各项措施和管理手段的正确实施，使网络系统信息数据的机密性、完整性及可用性受到全面、可靠的保护。

7.3.1　信息安全策略管理的挑战和需求分析

在企业信息安全管理体系的建设过程中，基于企业的实践经验和教训，企业管理层逐步认识到信息安全策略的建立和执行是安全管理体系建设中的关键环节，是企业合规管理和管理体系执行效率的集中体现。企业信息安全策略在整个信息安全管理体系中是执行部分，是企业信息安全管理体系建设的实体。如果没有信息安全策略的制定与执行，企业信息安全方针、目标、制度就是一纸空文，信息安全技术与设备就是摆设。

7.3.2　信息安全策略概述

信息安全策略是企业管理层解决信息安全问题最重要的部分。具体讲是一组规则，它们定义了企业要实现的安全目标和实现这些安全目标的途径。信息安全策略可以划分为两个部分：问题策略和功能策略。问题策略描述了一个组织所关心的安全领域和对这些领域内安全问题的基本态度。功能策略描述如何解决所关心的问题，包括制定具体的硬件和软件配置规格说明、使用策略以及员工行为策略。信息安全策略必须有清晰和完全的文档描述，必须有相应的措施保证信息安全策略得到强制执行。在组织内部，必须有行政措施保证制定的信息安全策略被不打折扣地执行，管理层不能允许任何违反组织信息安全策略的行为存在，另一方面，也需要根据业务情况的变化不断地修改和补充信息安全策略。

在企业组织内部，信息安全策略的制定者一般应该是该组织的技术管理者，可能是由一个多方人员组成的小组。信息安全策略反映出企业对现实和未来安全风险的认识水平，对组织内部业务人员和技术人员安全风险的假定与处理，同时还需要参考相关的标准文本和类似组织的安全管理经验。

信息安全策略的内容应该有别于技术方案，信息安全策略只是描述企业保证信息安全的途径的指导性文件，它不涉及具体做什么和如何做的问题（操作规程问题），只需指出要完成的目标。信息安全策略是原则性的，不涉及具体细节，对整个组织提供全局性指导，为具体的安全措施和规定提供一个全局性框架。在信息安全策略中不规定使用什么具体技术，也不描述技术配置参数。信息安全策略的另外一个特性就是可以被审核，即能够对组织内各个部门信息安全策略的遵守程度给出评价。

信息安全策略的描述语言应该是简洁的、非技术性的和具有指导性的。比如一个涉及对敏感信息加密的信息安全策略条目可以这样描述：

条目 1 “任何类别为机密的信息，无论存储在计算机中，还是通过公共

网络传输时，必须使用本公司信息安全部门指定的加密硬件或者加密软件予以保护。”

这个叙述没有谈及加密算法和密钥长度，所以当旧的加密算法被替换，新的加密算法被公布的时候，无须对信息安全策略进行修改。

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则，它包括以下三个重要的组成部分。①依据：企业信息安全的基石是社会法律、法规与手段、制度。通过建立一套安全管理标准和方法，可以使非法者慑于法律，不敢轻举妄动。②技术：先进的安全技术是信息安全的根本保障。企业通过对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。③管理：各网络使用机构、企业和单位应建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

安全策略是指某个安全区域内用于所有与安全有关的活动的规则，分三级：安全策略目标、机构安全策略、系统安全策略。

7.3.3 信息安全策略工作

企业信息安全策略工作主要从两方面进行，一是企业信息安全策略的制定，二是企业信息安全策略的贯彻、执行。

1. 企业信息安全策略制定的内容

1）制定安全策略的原则

（1）适应性原则：在一种情况下实施的安全策略到另一环境下就未必适合。

（2）动态性原则：用户在不断增加，网络规模在不断扩大，网络技术本身的发展变化也很快。

（3）简单性原则：安全的网络是相对简单的网络。

（4）系统性原则：应全面考虑网络上各类用户、各种设备、各种情况，有计划有准备地采取相应的策略。

（5）最小特权原则：每个用户并不需要使用所有的服务；不是所有用户都需要去修改系统中的每个文件；每个用户并不需要都知道系统的根口令，每个系统管理员也没有必要都知道系统的根口令等。

2）制定安全策略的思想方法

（1）凡是没有明确表示允许的就要被禁止。

例如，如果决定某一台机器可以提供匿名 FTP 服务，那么可以理解为除了匿名 FTP 服务之外的所有服务都是禁止的。

（2）凡是没有明确表示禁止的就要被允许。

例如，如果决定某一台机器禁止提供匿名 FTP 服务，那么可以理解为除了匿名 FTP 服务之外的所有服务都是允许的。

这两种思想方法所导致的结果是不相同的。第一种思想方法所表示的策略只规定了允许用户做什么，而第二种思想方法所表示的策略只规定了用户不能做什么。网络服务类型很多，新的网络服务功能将逐渐出现。因此，在一种新的网络应用出现时，对于第一种思想方法，如允许用户使用，就将明确地在安全策略中表述出来；而按照第二种思想方法，如果不明确表示禁止，就意味着允许用户使用。

需要注意的是：在信息安全策略上，一般采用第一种思想方法，即明确地限定用户在网络中访问的权限与能够使用的服务。这符合于规定用户在网络访问的“最小权限”的原则，即给予用户能完成他的任务所“必要”的访问权限与可以使用的服务类型，这样将会便于网络的管理。

3）安全策略的设计依据

制定信息安全策略应考虑以下因素：

（1）对内部用户和外部用户分别提供哪些服务程序；

（2）初始投资额和后续投资额（新的硬件、软件及工作人员）；

（3）方便程度和服务效率的平衡；

（4）复杂程度和安全等级的平衡；

（5）网络性能。

4）安全策略的对象范围

安全策略制定的过程中，首先要对所有信息化资源从安全性的角度去定义它所存在的风险。第一步要分析在所要管理的网络中有哪些资源，其中哪些资源是重要的，什么人可以使用这些资源，哪些人可能会对资源构成威胁，以及如何保护这些资源。设计网络安全策略的第一步工作是研究这些问题，并将研究结果用网络资源调查表的形式记录下来。要求被保护的网络资源被定义之后，就需要对可能对网络资源构成威胁的因素下定义，以确定可能造成信息丢失和破坏的潜在因素，确定威胁的类型。只有了解了对网络资源安全构成威胁的来源与类型，才能针对这些问题提出保护方法。

RFC 文档 1044 列出了以下需要定义的网络资源：

（1）硬件：处理器、主板、键盘、终端、工作站、个人计算机、打印机、磁盘、通信数据、终端服务器与路由器。

（2）软件：操作系统、通信程序、诊断程序、应用程序与网管软件。

（3）数据：在线存储的数据、离线文档、执行过程中的数据、在网络中传输的数据、备份数据、数据库、用户登录。

（4）用户：普通网络用户、网络操作员、网络管理员。

（5）演示程序：应用软件的演示程序、网络操作系统的演示程序、计算机硬件与网络硬件的演示程序与网络软件的演示程序。

（6）支持（外部）设备：磁带机与磁带、软盘、光驱与光盘。

5）安全威胁与风险分析

为了保护计算机系统和网络必须对潜在的安全威胁提高警惕。如果理解了

安全的确切定义，就能很敏感地对计算机系统和网络进行风险评估。要进行有效的安全评估，就必须明确安全威胁、漏洞的产生，以及威胁、安全漏洞和风险三者之间的关系。安全威胁：威胁是有可能访问资源并造成破坏的某个人、某个地方或某个事物。目前有以下安全威胁：

（1）内部窃密和破坏；

（2）窃听和截收；

（3）非法访问（以未经授权的方式使用网络资源）；

（4）破坏信息的完整性（通过篡改、删除和插入等方式破坏信息的完整性）；

（5）冒充（攻击者利用冒充手段窃取信息、入侵系统、破坏网络正常通信或欺骗合法主机和合法用户）；

（6）流量分析攻击（分析通信双方通信流量的大小，以期获得相关信息）；

（7）其他威胁（病毒、电磁泄漏、各种自然灾害、战争、失窃、操作失误等）。

6）安全等级的确定

目前企业可采用的信息安全等级与标准一般是由国家相关部门制定的适合我国企业发展和国家安全的标准。我国目前执行的等级标准有等级保护的相关标准和涉密信息系统分级保护的相关标准。企业根据合规要求、市场要求或企业自身需求，明确企业需要遵从的安全等级。

7）制定安全策略的内容

制定安全策略的目的是保证网络安全，保护工作的整体、计划性及规范性，保证各项措施和管理手段的正确实施，使网络系统信息数据的机密性、完整性及可使用性受到全面、可靠的保护。其包括以下内容：

（1）进行安全需求分析；

（2）对网络系统资源进行评估；

（3）对可能存在的风险进行分析；

（4）确定内部信息对外开放的种类及发布方式和访问方式；

（5）明确网络系统管理人员的责任和义务；

（6）确定针对潜在风险采取的安全保护措施的主要构成方面，制定安全存取、访问规则。

2．执行信息安全策略的过程

1）确定应用范围

在制订安全策略之前一个必要的步骤是确认该策略所应用的范围，如是在整个组织还是在某个部门。如果没有明确范围就制订策略无异于无的放矢。

2）获得管理支持

事实上任何项目的推进都无法离开管理层的支持，安全策略的实施也是如此。先从管理层获得足够的承诺有很多好处，可以为后面的工作铺平道路，还可以了解组织总体上对安全策略的重视程度，而且与管理层的沟通也是将安全

工作进一步导向更理想状态的一个契机。

3）进行安全分析

安全分析是一个经常被忽略的工作步骤，同时也是安全策略制订工作中的一个重要步骤。这个步骤的主要目标是确定需要进行保护的信息资产，及其对组织的绝对和相对价值，在决定保护措施的时候需要参照这一步骤所获得的信息。进行这项工作时需要考虑的关键问题包括需要保护什么，需要防范哪些威胁，受到攻击的可能性，在攻击发生时可能造成的损失，能够采取什么防范措施，防范措施的成本和效果评估等等。

4）会见关键人员

通常来说至少应该与负责技术部门和负责业务部门的人员进行一些会议，在这些会议上应该向这些人员灌输在分析阶段所得出的结论并争取这些人员的认同。如果有其他属于安全策略应用范围内的业务单位，那么也应该让其加入到这项工作。

5）制定策略草案

一旦就应用范围内采集的信息达成一致并获得了组织内部足够的支持，就可以开始着手建立实际的策略了。这个策略版本会形成最终策略的框架和主要内容，并作为最后评估和确认工作的基准。

6）开展策略评估

在之前已经与管理层及安全策略执行相关的主要人员进行了沟通，而该部分工作在之前的基础上进一步与所有风险承担者一同对安全策略进行确认，从而最终形成修正后的正式的策略版本。在这个阶段往往会有更多的人员参与进来，应该进一步争取所有相关人员的支持，至少应该获得足够的授权以保障安全策略的实施。

7）发布安全策略

当安全策略完成之后还需要在组织内成功地进行发布，使组织成员仔细阅读并充分理解策略的内容。可以通过组织主要的信息发布渠道对安全策略进行广泛发布，如组织的内部信息系统、例会、培训活动等。

8）修订策略

随着应用环境的变化，信息安全策略也必须随之变化和发展才能继续发挥作用。通常组织应该每季度进行一次策略评估，每年至少应该进行一次策略更新。

7.4　信息安全风险管理

企业信息安全风险管理是信息安全管理体系中检查信息安全策略执行、明确合规要求的必要手段。企业信息安全风险管理是一个动态的、循环的过程，是建立在风险识别、风险分析、风险评估的基础上，还要对风险控制措施加以

落实，并进行有效的监督和控制。企业信息安全不是绝对的，在企业实施信息安全风险管理的同时，还需要参照成本、效益的原则，有效地整合企业各种资源。

7.4.1 信息安全风险管理的挑战和需求分析

现代企业能否有效地对风险进行全面的管理，是企业竞争力高低、决定其经营能力高低的关键和核心。也就是企业能否积极主动地承担风险、管理风险、建立良好的风险管理架构和体系，以良好的风险定价策略获得利润。因此，对于企业而言，全面风险管理是内部管理的核心，在整个管理体系中的地位已上升到企业发展战略的高度。企业信息安全风险管理是企业全面风险管理的重要内容。企业规范风险评估工作，是提高企业信息安全风险管理水平，促进业务安全、持续、稳健发展，促进合规管理、组织机构建设、制度建设、策略建设、运维建设、技术架构建设的关键。

企业可以参照 ISO 13335 等国际、国内标准来组织、制定各个企业的信息安全风险管理的相关流程，但是由于各个企业业务类型的不同，风险管理的策略与方法也不尽相同。特别是风险评估的方法与流程，这是企业信息安全风险管理中最大的挑战。

7.4.2 信息安全风险概述

企业信息安全风险，是指企业信息化在合规管理、支持业务创新和业务运营过程中，由于管理流程及资源缺失或不足、自然因素、人为因素和技术漏洞产生的操作、法律、声誉等风险。企业信息安全风险管理是对企业信息安全风险进行识别、评价、处置、整改等的全过程。风险管理应遵循“全面覆盖、突出重点、持续跟进”的原则。其中风险评估是识别、计量、评价信息安全风险的活动，是风险管理中的关键环节，风险评估对象包括信息科技组织、管理过程和信息资产。

7.4.3 信息安全风险管理工作内容

1. 风险管理工作的内容

企业信息安全风险管理工作主要有风险评估、处置与整改，包括以下工作内容：

1）确定范围和方针

信息安全风险管理可以覆盖企业的全部或者部分。无论是全部还是部分，组织都必须明确界定风险管理的范围，并且文件化信息安全风险管理范围。

2）定义风险评估的系统性方法

确定信息安全风险评估方法，并确定风险等级准则。评估方法应该和企业既定的信息安全管理体系范围、信息安全需求、法律法规要求相适应，兼顾效果和效率。建立风险评估文件，解释所选择的风险评估方法、说明为什么该方法适合组织的安全要求和业务环境，介绍所采用的技术和工具，以及使用这些技术和工具的原因。评估文件还应该规范下列评估细节：

（1）信息安全管理体系内资产的估价，包括所用的价值量化信息；

（2）威胁及薄弱点的识别；

（3）可能利用薄弱点的威胁的评估，以及此类事故可能造成的影响；

（4）以风险评估结果为基础的风险计算，以及剩余风险的识别。

3）识别风险

识别信息安全管理体系控制范围内的信息资产；识别对这些资产的威胁；识别可能被威胁利用的薄弱点；识别保密性、完整性和可用性丢失对这些资产的潜在影响。

4）评估风险

根据资产保密性、完整性或可用性丢失的潜在影响，评估由于安全失败可能引起的商业影响；根据与资产相关的主要威胁、薄弱点及其影响，以及目前实施的控制，评估此类失败发生的现实可能性；根据既定的风险等级准则，确定风险等级。

5）识别并评价风险处理的方法

对于所识别的信息安全风险，组织需要加以分析，区别对待。如果风险满足组织的风险接受方针和准则，那么就有意地、客观地接受风险；对于不可接受的风险组织可以考虑避免风险或者转移风险；对于不可避免也不可转移的风险应该采取适当的安全控制，将其降低到可接受的水平。

6）为风险的处理选择控制目标与控制方式

选择并文件化控制目标和控制方式，以将风险降低到可接受的等级。ISO 27002 附录 A 提供了可供选择的控制目标与控制方式。不可能总是以可接受的费用将风险降低到可接受的等级，那么需要确定是增加额外的控制，还是接受高风险。在设定可接受的风险等级时，控制的强度和费用应该与事故的潜在费用相比较。这个阶段还应该策划安全破坏或违背的探测机制，进而安排预防、制止、限制和恢复控制。在形式上，组织可以通过设计风险处理计划来完成步骤 5 和 6。风险处理计划是组织针对所识别的每一项不可接受风险建立的详细处理方案和实施时间表，是组织安全风险和控制措施的接口性文档。风险处理计划不仅可以指导后续的信息安全管理活动，还可以作为与高层管理者、上级领导机构、合作伙伴或者员工进行信息安全事宜沟通的桥梁。这个计划至少应该为每一个信息安全风险阐明以下内容：组织所选择的处理方法；已经到位的控制；建议采取的额外措施；建议的控制的实施时间框架。

7）获得最高管理者的授权批准

剩余风险的建议应该获得批准，开始实施和运作信息安全管理体系需要获得最高管理者的授权。

风险评估流程如图 7-1 所示。

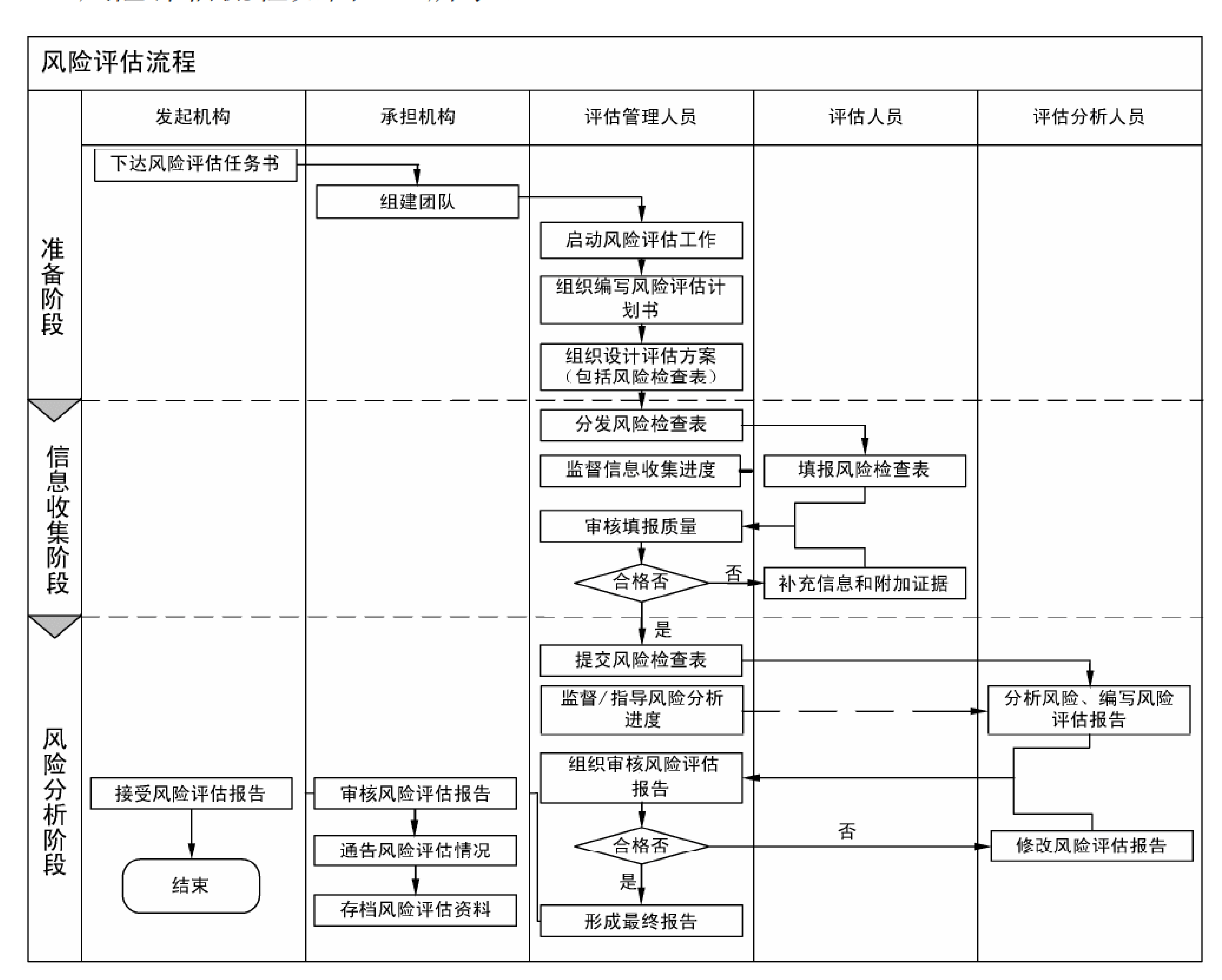


图 7-1 企业信息安全风险评估流程

2. 风险评估工作的主要内容

1）成立组织结构或职责分工

发起并指定承担机构，承担机构负责组建风险评估实施团队。风险评估实施团队由管理层、相关业务和技术骨干等人员组成，评估工作角色分为：评估管理人员、评估人员、评估分析人员。

评估管理人员负责组织、管理、监督风险评估任务，包括以下内容：

（1）制定风险评估任务计划；

（2）设计风险评估方案；

（3）审核风险评估报告；

（4）确认风险处置建议；

（5）跟踪风险评估任务进度；

（6）控制风险评估任务质量。

评估管理人员由承担机构管理人员担任，也可委派信息安全管理人员担任。

评估人员负责按照风险评估任务要求，收集并提供信息和证据，如实反映信息化工作现状。评估人员由评估对象所涉及的相关技术或业务骨干人员担任。

评估分析人员负责汇总、整理和分析采集到的信息与证据材料，编写风险评估报告。评估分析人员由行内专业人员担任，必要时可聘请业内专业人员。

在同一风险评估任务中，评估实施团队成员不少于三人，评估管理人员和评估分析人员不得兼任评估人员。

2）风险评估计划

风险管理部门开展整体信息科技风险评估，业务管理部门进行专项信息科技风险评估。

出现以下情况时，应结合本单位以往风险评估情况，确定是否启动专项信息科技风险评估。

（1）新系统上线或已有系统进行重大变更；

（2）信息科技运行中发现重大纰漏或隐患；

（3）内部或同业出现重大信息科技事件；

（4）信息科技审计中发现重大问题；

（5）监管机构发布风险提示；

（6）其他情况。

3）风险评估方法

风险评估通过人工评估或自动化工具测评等手段识别、分析支撑 IT 目标的流程和资源中存在的缺失或不足，判断风险优先级，提出风险处置建议。

评估管理人员组织评估团队识别所评估对象的 IT 服务目标，进而分析支撑 IT 目标的流程和资源；识别影响流程和资源中的关键因素，主要考虑各流程要素的活动内容、关联关系、流程目的、实现方式、所需资源等；根据关键因素设计风险检查项、检查指标和评价权重，形成风险检查表。

评估人员依据风险检查表，采用人工或自动化工具对评估对象的信息科技状况进行信息收集。信息收集可采用调查、检查、安全测试等方式。

（1）调查包括问卷调查、远程访谈、现场访谈等；

（2）检查包括文档检查、代码检查、流程检查等；

（3）安全测试包括人工测试、自动化测试以及综合性渗透测试等。

评估分析人员采用定性或定量的计算方法，依据各类风险对实现 IT 目标的影响，计算出评估对象的风险优先值或级别，并进行以下分析：

（1）风险成因分析：分析诱发风险的主观因素和客观因素。主观因素包括流程缺失、控制不足或无效等；客观因素包括资源缺乏、内外环境影响等。

（2）风险占比分析：依据对 IT 目标的影响程度，分析评估对象当前状态下

各类、各级风险占比情况。

（3）风险对比分析：对同次任务中不同机构的风险状态进行对比，分析各类风险在不同机构的分布状况及影响。

（4）风险趋势分析：对不同时期的相同任务结果进行对比，分析同一风险的增强或减弱情况，了解风险的发展趋势。

风险分析可采用专家经验、风险分析模型以及风险分析工具等手段。

评估分析人员针对风险评估任务中揭示的风险类型和状态，结合组织机构、业务需求和安全要求，提出风险处置建议，包括预防、降低、转移或消除风险的措施、预期效果等。

评估分析人员编写风险评估报告，内容包括风险评估任务描述、风险分析、风险处置建议等。

4）风险评估准备

根据风险评估计划，风险管理部门提出风险评估任务，编制风险评估任务书，明确任务目标、评估对象、评估范围、任务起止时间、任务承担机构等。风险评估任务书经发起机构负责人批准后发布。

任务承担机构组建风险评估团队，指定风险评估管理人员、风险评估人员和风险评估分析人员，并授权风险评估团队开展风险评估工作。

评估管理人员组织制定风险评估任务计划书，明确风险评估实施活动的计划安排，主要包括：

（1）团队组织：包括成员名单、角色、职责等内容；

（2）工作计划：描述各阶段的工作安排，包括工作内容、时间进度和各阶段成果清单等内容。

评估管理人员组织设计评估方案，评估方案包括风险检查表、信息收集方式、风险分析方法等，通过风险评估启动会等形式启动具体风险评估工作。

5）信息收集

评估管理人员将风险检查表分发给评估人员，并告知信息收集方法及填写要求。通过调阅文档、收集日志、现场访谈、工具测评等方式获取风险评估所需信息。信息内容包括但不限于：IT 制度及执行情况、技术文档、以往审计报告、风险管理报告、日志记录、访谈记录、测试报告等。

评估人员根据采集的信息，填写风险检查表，并保留证据。

评估管理人员督查信息收集进展情况，按计划收回风险检查表，并审核填报信息质量。必要时，可要求评估人员补充信息和附加证据，然后将风险检查表提交评估分析人员。

6）风险分析

评估分析人员按评估方案确定的风险分析方法对风险检查表进行汇总、梳理，评定风险等级，分析风险成因，提出风险处置建议，形成风险评估报告。报告包括但不限于以下内容：

（1）风险评估任务概述；

（2）风险评估活动描述；

（3）风险分析，包括总体风险分析、风险占比分析、风险对比分析、风险趋势分析；

（4）风险成因分析；

（5）风险处置建议；

（6）详细风险列表。

评估分析人员将风险评估报告提交评估管理人员。评估管理人员督查风险分析进展情况，指导风险分析工作，组织审核风险评估报告，形成正式报告并提交任务承担机构。

任务承担机构将风险评估报告上报任务发起机构，并通过风险评估任务总结会等形式，通报风险评估情况。任务承担机构将风险评估资料归档管理。

第8章

信息安全运维体系

企业信息安全运维与安全组织联系紧密，融合在业务管理和 IT 管理体系中。安全运维包含威胁分析与预警、安全状态和事件的监控、安全事件或事故的响应，以及基于安全目标的操作行为和日志审计，这些安全运维的任务主要可通过安全事件监控、响应、审计和相应的安全策略体系共同完成。本章从信息安全事件的监控、响应、审计，以及信息安全外包服务四个维度进行企业信息安全运维体系构建描述。

8.1 概述

通常企业信息安全运维包含两层含义：一是企业在信息安全运维过程中，对企业网络或系统发生病毒或黑客攻击等安全事件进行定位、防护、排除等运维动作，保障系统不受内、外界侵害；二是企业在对安全运维过程中发生的基础环境、网络、安全、主机、中间件、数据库乃至核心应用系统发生的影响其正常运行的事件（包含关联事件）通称为安全事件，以及围绕安全事件、运维人员和信息资产，依据具体流程而展开监控、响应、审计、评估等运行维护活动。

目前大多数企业信息安全运维服务还停留在被动的、传统意义上的安全运维管理，其存在很多弊端，主要表现在以下三个方面：

1．混乱的措施与管理

企业在发生安全事件、故障时，即使有众多的专业安全厂商管理工具，却无法迅速定位安全事件，更无法快速进行安全事件响应处理，时时处于混乱，无序的运维管理状态，无法提供可量化的安全运维管理制度及规范。

2．匮乏的经验与方法

企业的信息系统运维与管理仍在依靠各自的“业务骨干”支撑，缺少相应的流程和经验积累，也没有完善的安全运维方针、策略、方法，过多依赖于人。

3．缺失的分析与评估

对安全事件缺少关联性分析和评估分析，并且没有对安全事件定义明确的

处理流程，更多的是依靠人的经验和责任心，缺少必要的审核和工具的支撑。

正是因为目前运维中存在的弊端，企业需要依靠长期从事信息系统运维的经验，同时结合信息安全保障体系建设中运维体系建设的要求，遵循 ITIL（最佳实践指导）ISO/IEC 27000 系列服务标准、等级保护和分级保护制度，建立一整套信息安全运维管理体系。

8.1.1　运维监控中心

基于关键业务点面向业务系统可用性和业务连续性进行合理布控和监测，以关键绩效指标指导和考核信息系统运行质量和运维管理工作的实施和执行，建立全面覆盖信息系统的监测中心，并对各类事件作出快速、准确的定位和展现，实现对信息系统运行动态的快速掌握，以及运行维护管理过程中的事前预警、事发时快速定位。运维监控中心主要包括：

1. 集中监控

企业采用开放的、遵循国际标准的、可扩展的架构，整合各类监控管理工具的监控信息，实现对信息资产的集中监视、查看和管理的智能化、可视化监控系统。监控的主要内容包括基础环境、网络、通信、安全、主机、中间件、数据库和核心应用系统等。

2. 综合呈现

企业可以合理规划与布控，整合来自各种不同的监控管理工具和信息源，进行标准化、归一化的处理，并进行过滤和归并，实现集中、综合的展现。

3. 快速定位和预警

企业的信息管理人员经过同构和归并的信息，将依据预先配置的规则、事件知识库、关联关系进行快速的故障定位，并根据预警条件进行预警。

8.1.2　运维告警中心

运维告警中心基于规则配置和自动关联，实现对监控采集、同构、归并信息的智能关联判别，并综合地展现信息系统中发生的预警和告警事件，帮助运维管理人员快速定位、排查问题所在。同时，告警中心提供多种告警响应方式，内置与事件响应中心的工单和预案处理接口，可依据事件关联和响应规则的定义，触发相应的预案处理，实现运维管理过程中突发事件和问题处理的自动化和智能化。其中主要包括：

1. 事件知识库维护

事件知识库维护是事件知识库的基础功能，内置大量的标准事件，按事件

类型进行合理划分和维护管理，可基于事件名称和事件描述信息进行归一化处理的配置，定义了多源、异构信息的同构规则和过滤规则。

2．智能关联分析

智能关联分析借助基于规则的分析算法，对获取的各类信息进行分析，找到信息之间的逻辑关系，结合安全事件产生的网络环境、资产重要程度，对安全事件进行深度分析，消除安全事件的误报和重复报警。

3．综合查询和展现

综合查询和展现实现了多种视角的故障告警信息和业务预警信息的查询和集中展现。

4．告警响应和处理

告警响应和处理提供了事件生成、过滤、短信告警、邮件告警、自动派发工单、启动预案等多种响应方式，内置监控界面的图形化告警方式；提供了与事件响应中心的智能接口，可基于事件关联响应规则自动生成工单并触发相应的预案工作流进行处理。

8.1.3 事件响应中心

事件响应中心借鉴并融合了 ITIL（信息系统基础设施库）/ITSM（IT 服务管理）的先进管理规范和最佳实践指南，借助工作流模型参考等标准，开发图形化、可配置的工作流程管理系统，将安全运维管理工作以任务和工作单传递的方式，通过科学的、符合用户安全运维管理规范的工作流程进行处置，在处理过程中实现电子化的自动流转，无需人工干预，缩短了流程周期，减少人工错误，并实现对安全事件、问题处理过程中的各个环节的监控和审计。

1．图表式的工作流建模

企业需要实现对安全运维措施、流程建模的图形化管理，同时需要进行易用的运维措施的创建和维护，以及简洁的工作流程，规范的仿真和验证。

2．定制化的运维流程

企业所有运维管理流程均可由用户自行配置定义，既可实现 ITIL/ITSM 的主要运维管理流程，又可根据用户的实际业务信息安全运维管理要求和规范，配置个性化的任务、事件处理流程。

3．灵活的自动派单

灵活的自动派单是指灵活、多样的规则匹配和处理，企业基于用户管理规范的自动处理，降低事件、任务发起到处理的延时，以及人工派发的误差。

4．全面的事件响应监控

企业需要实现对安全事件响应处理全过程的跟踪记录和监控，根据 ITIL 管理建议和用户运维要求，对安全事件响应处理的响应时限和处理时限进行监督和监管。

5．安全事件响应处理知识库

企业需要累积各类安全事件响应处理，并建立自有的知识库，实现对事件处理过程的备案和综合查询，帮助用户在处理事件时查找历史处理记录和流程，为企业信息安全运维管理工作积累经验。

8.1.4　安全事件审计评估中心

安全事件审计评估中心提供对信息系统运行质量、服务水平、安全运维工作绩效的综合评估、考核、审计管理的功能。

1．安全事件评估

安全事件评估遵循国际和工业标准及指南建立平台的运行质量评估框架，通过评估模型使用户了解运维需求、认知运行风险、采取相应的保护和控制，有效地保证信息系统的建设投入与运行风险的平衡，系统地保证信息化建设的投资效益，提高关键业务应用的连续性。

2．安全运维考核

安全运维考核是为了在评价过程中避免主观臆断和片面随意性，进而实现工作量、工作效率、处理考核、状态考核等功能。

3．安全事件审计

安全事件审计是以跨平台多数据源信息安全审计为框架，以电子数据处理审计为基础的信息审计系统。其主要包括系统流程和输入输出数据以及数据接口的完整性、合规性、有效性、真实性审计。

8.1.5　安全运维管理核心

企业 IT 资产管理是全面实现信息系统运行维护管理的基础，安全运维管理的核心也是信息资产管理，提供对企业丰富的 IT 资产信息属性维护和备案管理，以及对网络和业务应用系统的备案和配置管理。基于关键业务点配置关键业务的基础设施关联，通过资产对象信息配置丰富业务应用系统的运行维护内容，实现各类 IT 基础设施与用户关键业务的有机结合，以及全面的综合监控。

1. 安全态势感知

安全态势感知是指全面整合现有各类设备和系统的各类异构信息，包括网络设备、安全设备、应用系统和终端管理中各种事件，经过分析后的综合展现界面，注重对信息系统的运行状态、综合态势的宏观展示。

2. 统一采集管理

企业以信息系统内各种 IT 资源及各个核心业务系统的监控管理为主线，采集相关异构监控系统的信息，通过对不同来源的信息数据的整合、同构、规格化处理、规则匹配，生成面向运行维护管理的事件数据，实现信息的共享和标准化。

3. 统一配置管理

企业从系统容错、数据备份与恢复和运行监控三个方面着手建立自身的运行维护体系，采用统一管理配置平台监测器实时监测与运行检测工具主动检查相结合的方式，构建一个安全稳定的系统。

8.2 安全事件监控

谈到安全事件监控，往往让人首先想到的就是摄像头、监视器等等，对于企业安全事件监控，不仅仅涉及物理环境与人员的安全监控，更多的是针对企业网络与业务系统的安全事件监控，企业网络与业务系统信息化建设不断完善，使得各类信息安全事件成为企业发展必须面对的问题，甚至各类严重的安全事件直接关系到企业的生死存亡。信息安全事件监控是企业及时响应与解决各类安全事件的前提。

企业信息安全事件监控的目的是为了预防内部各业务系统由于权限滥用或者管理不当所导致网络信息安全事件发生，保护并及时处理由此引发的各类信息安全事件，降低或者避免突发安全事件造成的经济损失与社会影响，保障企业网络与业务系统正常运行。

8.2.1 概述

安全事件监控的重要功能需求主要包括安全事件的收集、安全事件的归并和过滤、安全事件标准化、安全事件显示和报表。

在企业的信息系统中，存在大量的 IT 资源，这些资源在实际运行中每时每刻都在产生各种类型的事件信息，在这些事件信息中，安全事件是需要安全运维人员重点关注的内容。通过安全事件监控，可以帮助企业积极监控整个组织内的 IT 资源，过滤并关联事件，迅速定位安全威胁，并为安全事件响应提

供支持。

但是，企业信息系统中的安全事件类型复杂、数量较大，如何快速地识别和过滤出有效的安全威胁信息，是企业安全运维人员需要重点考虑的问题。在具体的信息安全系统中，安全事件监控的内容主要包括安全事件的收集、安全事件的归并和过滤、安全事件标准化、安全事件显示和报表等。安全事件监控大多通过单一安全控制台，集中地管理安全事故和漏洞，为企业用户提供安全架构的总体视图，使企业用户能够深入研究网络拓扑，了解受影响的资源的位置并判断问题的真正根源。

8.2.2　面临的挑战与需求分析

随着信息技术的迅猛发展和信息化的不断建设应用，企业在信息安全管理经营模式上逐步由传统模式向信息化管理模式转变。特别是全国性的大型企业集团网络，其业务信息系统网络由总部核心区、对外服务区、总部办公区、各个地市分支办公局域网、分支业务网等共同组成。企业在网络中部署了大量的不同厂家不同型号的网络设备（如路由器、交换机）、安全设备（如防火墙、入侵检测系统 IDS 等）和业务生产系统（如数据库系统、中间件系统）以及各种自动化办公系统等等。

同时，随着企业信息化建设不断完善，大量应用信息系统相继上线，整个应用信息系统面临的各种安全风险也日益严重，如何确保信息系统安全运行，降低运维管理成本，完善安全事件监控，已经成为企业信息系统建设过程中面临的主要问题。目前企业面对安全事件监控需求主要有以下几点：

1．解决因网络规模庞大，监控范围难以覆盖的问题

规模庞大企业广域网，部署大量网络设备、安全设备与应用系统，网络与设备环境情况极其复杂，并且企业网络规模随着业务扩展越来越大，如何进行高效安全事件监控，加强管理者对企业网络信息系统的整体运行状况了解，是亟待解决的问题。

2．如何对安全事件进行风险评估、分析

企业网络与设备因各种问题产生的海量安全事件，如何能够及时诊断快速定位，避免影响企业信息应用系统正常进行。

3．多样的安全事件如何归一化，实现全网监控

企业信息化安全建设阶段，以及异构安全性考虑，在整个企业网络中存在大量的异构安全设备，不同安全事件归一化如何实现，如何打破各类安全设备的采用所形成的安全信息孤岛。企业信息安全事件监控需要具备全局观，需要实现对全网、各类业务系统的安全运行态势进行整体把控，从全局的角度综合考虑安全风险。

监控中心实现一个安全可管理、运维的平台。实现类似网管系统的运维人员对网络设备的管理、运维与故障响应一样，使管理层、业务人员、技术人员都可以在安全运营中心系统里找到自己关心的安全信息。

8.2.3 安全事件监控的主要工作

安全事件监控的一个核心问题是如何对采集到的各类安全监控事件进行风险评估，划分出事件的安全风险级别，使得安全管理员能够根据事件的风险级别确定事件处理的优先级，按照轻重缓急的策略来协调资源并处理各类安全事件，从而实现信息系统整体安全风险管理和风险控制的目的。安全事件监控的运转流程是由系统运行时产生的事件日志生成、采集、分析的。要做到有效的安全事件监控，安全事件监控信息源是重要的先决条件，即风险管理中对于安全事件风险等级的识别和判定。

1. 安全事件监控数据呈现

安全事件监控需要综合建立统一管理平台，企业管理人员和维护人员在日常工作中，通过统一管理平台的操作管理界面，实现安全事件监控摘要信息、安全指标数据、统计分析数据的集中呈现界面，是平台的入口和工作平台页面。平台通过趋势图、汇总表、地图、网络图等形式，为管理者提供基于地理位置、网络拓扑、统计表格、监控对象、技术趋势指标等各类形式的呈现方式。

2. 安全事件归一化

安全事件监控的统一管理平台在收集到海量的安全事件后，必然需要进行安全事件归一化处理。来自不同设备和系统的安全事件千差万别，只有将这些大量的异构数据转化为平台内部统一的数据格式才能进行后续的安全事件关联分析，以及风险评估，才能为企业提供一个全局统一的事件监控界面。

3. 安全事件关联分析

安全事件关联分析实现海量安全事件的抽取、降噪，剥离无用信息，为企业提升后续安全管理工作的效率，降低安全事件监控管理工作的复杂性。安全事件关联分析是风险评估的基础，关联分析的结果导出的关联事件可以提升为威胁，从而参与风险评估的计算，并且实现风险计算自动化、定量化。

4. 安全事件管理

安全事件管理是一种实时的、动态的管理模型，通过安全事件监控统一平台进行安全事件收集、安全事件标准化、安全事件过滤、安全事件归并和安全事件关联后分析来自于不同地点、不同层次、不同类型的信息事件，帮助我们发现真正关注的安全风险，且提高安全报警的信噪比，从而可以准确地、实时地评估当前的安全态势和风险，并根据预先制定的策略作出快速的响应。

5. 安全事件预警

安全事件预警是根据来自内部预警信息、外部预警信息分析获得对可能发生的威胁的提前通告，提供各类安全威胁、安全风险、安全态势、安全隐患等信息，该模块提供规则设定功能，以便准确定位用户所关心的安全问题，以便有针对性地进行响应处理。

6. 安全事件知识库管理

企业通过安全事件监控，可以不断积累各类安全事件，并建立企业自有的安全事件知识库集合，实现安全事件信息的共享和利用，提供了一个集中存放、管理、查询安全知识的环境。建立企业处理的安全事件方法和应急方案，将标准漏洞信息和标准事件信息收集起来，形成安全事件共享知识库。

7. 安全事件数据报表管理

企业需要对安全事件监控获得的各类安全事件信息进行报表统计管理，是对各类安全运行数据的统计、挖掘、分析的呈现。通过各种形式化、标准化的报表报告实现对数据结果的展现，满足企业在安全法规遵从建设需求。

8.3 安全事件响应

事件响应的开始是因为有“事件”发生，所谓“事件”指的是那些影响企业正常运转的不当行为，或者危害企业利益的破坏行为。企业安全事件造成的损失往往是巨大的，而且往往是在很短的时间内造成的。因此，安全事件应急响应的关键是速度与效率。

安全事件响应是根据当前的安全事件监控，以及后续风险评估，及时调动有关资源作出响应，降低潜在的安全威胁对企业网络与应用信息系统的负面影响，实现了安全事件监控从采集、处理、告警到人工运维处理的自动化和流程化管理。对安全事件风险进行预警通知，并在安全事件响应模块里进行响应处理，实现了安全风险与安全事件响应的紧密联系。

8.3.1 概述

所谓安全事件应急响应，通常指企业为了应对各种意外事件的发生所做的准备以及在事件发生后所采取的措施。在本节中，安全事件的应急响应指的是应急响应组织根据事先对各种可能情况的准备，在安全事件发生后，响应、处理、恢复、跟踪的方法及过程。下面依次简述安全事件应急响应的对象、作用、行为和必要性。

1．安全事件应急响应的对象

安全事件应急响应的对象泛指针对计算机和网络所处理的信息的所有安全事件，事件的主体可能来自人、故障、病毒与蠕虫或者自然灾害等。应急响应的对象广义上还包括扫描等所有违反安全政策的事件，它们也称为应急响应的客体。对于企业一般的应急响应过程中会出现至少三种角色：事件发起者、事件受害者和进行应急响应的人员，分别简称为“入侵者”、“受害者”和“响应者”。

2．安全事件应急响应的作用和行为

安全事件应急响应的作用主要表现在事先的充分准备和事件发生后采取的措施两个方面。一方面是事先的充分准备，企业信息安全管理体系中的安全培训、制定安全政策和应急预案以及风险分析等，安全技术上则要增加系统安全性，如备份、部署安全产品等。另一方面是事后采取的抑制、根除和恢复等措施，其作用在于让企业尽可能地减少损失或尽快恢复正常运行。

3．安全事件应急响应的必要性

安全事件应急响应是一种被动性的安全体系，是持续运行并由一定条件触发的体系。首先，发生过的安全事件已经给企业造成惊人的损失并显示出巨大的危害性，而且随着企业对网络和业务系统的依赖性增加，安全事件给企业造成的破坏也随之增大；其次，从企业信息安全管理的角度上考虑，并非所有的实体都有足够的实力进行信息安全管理。因此，作为补救性的安全事件应急响应是必不可少的。

8.3.2 需求分析

对于信息系统的安全而言，我们追求的是防患于未然而不是亡羊补牢，只要有可能，我们就应该尽可能地去主动防止安全事件的发生。然而，我们不可能预防所有的安全事件。一旦安全事件发生，我们首先要做的就是及时响应，将安全事件的影响最小化。对于这一点，仅仅依靠安全防护产品的自动化防御是不够的。比如，安全防护产品无法防止由于人为错误导致的安全事件。

由于信息系统及相关系统的复杂性和互相关联，为了实现有效的安全事件响应，必须考虑以下方面的工作制定安全事件响应计划、组建安全事件响应小组、确定团队人员角色等。另外，安全事件响应本身还有着突发性强，对处理人员的综合技术和专业能力要求高等特点，这些都对企业信息系统的管理者提出了不小的挑战。

企业在进行信息安全建设到一定阶段后，已经采购了大部分的安全产品并部署，然而网络中仍然存在比较多的安全问题，而这些安全问题导致已有的安全投资效果并不明显，无法解决企业网络中出现的安全事件，使得企业对安全

事件应急响应建设有了一定的要求，主要从以下四个方面分析：

1．如何快速响应突发的安全事件

企业部署的安全设备起不到应有的作用，无法全部解决网络中频繁出现的安全事件，企业网络中一旦出现安全事件时，企业安全管理人员不能及时发现，也无法及时处理。

2．如何建全响应措施，降低企业损失

企业安全管理人员无法全面了解整个企业网络中正在发生的内部越权访问和外部攻击，新出现的网络蠕虫病毒造成了较大的损失，甚至造成工作和业务的停顿，但无法根除，也缺少必要措施应对。

3．如何规范响应制度，实现响应专业化管理

在企业网络出现问题的情况下，企业安全管理人员无从下手或者手忙脚乱，也没有相应的机制、制度指导该如何处理，无法迅速查明真正的原因。

4．如何统筹全局，建立企业安全事件响应体系

企业各个单位各自为政，对遇到的安全问题无法进行统一考虑，导致同样的安全问题多次出现，同时缺少统一规范的快速处理措施及流程。各自为政的单位的随意性，使得企业无法建立统筹全局的安全事件响应体系。

8.3.3　安全事件响应的具体工作

为了能够合理、有序地处理安全事件，将安全事件响应划分为六个阶段：准备、检测、抑制、根除、恢复、追踪，企业可以根据响应政策对每个阶段定义适当的目的，明确响应顺序和过程。其中主要的响应步骤是抑制、根除和恢复，抑制的目的在于限制攻击范围，限制潜在的损失与破坏，在安全事件被抑制以后，应该尽快找出安全事件根源并彻底根除；然后进行网络和业务系统恢复，恢复的目的是把所有受侵害的业务系统、应用、数据库等恢复到正常的运行状态。

1．安全事件响应小组的创建与管理

对于保障企业信息系统的安全来说，不存在单一的解决方案，而需要一种多层次的安全管理策略。在这些安全层次当中，建立安全事件应急响应小组已经成为必要的工作了。响应小组的创建和管理对安全事件响应工作是非常重要的，许多事件响应工作的失败就是因为在创建和管理应急响应小组方面出现了问题。

2．制定标准的安全事件响应措施与流程

企业需要通过专业信息安全咨询，规范、标准化所有安全事件响应措施，以及安全事件响应流程，严格要求企业信息安全响应小组进行规范化的管理、运作。企业还需要统一规范安全事件报告格式，建立及时精确的安全事件上报体系，并在此基础上，进一步研究针对各类安全事件的响应对策，从而建立一个专业安全事件应急响应体系，完善安全事件应急响应知识库。

3．安全事件响应的具体工作步骤

（1）记录日志：当发生安全事件时，企业首先需要对环境现场进行记录，对事件的影响进行详细描述。安全事件日志对于安全事件的识别、处理和调查非常重要，安全事件可能在其刚刚发生时就暴露，也可能在发生的过程中或发生以后才被发现，因此所有安全事件都应该有一份书面的经过调查证明足够客观的日志，而且应该把日志妥善保存以免被修改。另一方面，在线日志很容易被修改和删除，手工记录是很有必要的。

（2）分析确认：企业根据记录的安全事件描述，结合前期进行过的安全检查、安全监控与审计，以及网络状况，进行分析和判断。也可以通过工具直接进行测试，结合当前扫描、探测、实时监控和审计的结果进行分析，可以更容易定位出问题所在。

（3）事件处理：事件响应最主要的任务之一就是维持或恢复组织的运作。因此，一旦发生意外事件，如何防止攻击或损害事件的扩大是其主要的目标，相关人员在现场或者远程依照不同事件类型进行事件处理。事件处理过程中，要对每个处理的动作进行详细记录。

（4）系统恢复：在处理了事件以后，就要对系统进行恢复，使企业业务重新运转。如果系统在故障点有备份，被攻击的系统就用备份来恢复；应该从系统中彻底删除诸如受到感染的文件；如果调整了网络或安全产品，要把所有安全上的变更做记录。

（5）事后分析与跟踪：在安全事件处理完毕，所有系统恢复正常以后，应该针对事件进行分析。集中企业所有相关人员来讨论所发生的安全事件以及得到的经验教训，对现有的一些流程进行重新评审，并对不适宜的环节进行修改。在安全事件处理后的一段时间内，企业应该密切关注系统恢复以后的安全状况，特别是曾经出问题的地方。

8.4 安全事件审计

安全审计一般是指由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权，对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价。由此来看，审计可以是来自内部的，也可以

是来自外部的。

安全事件审计来自企业内部，是对企业网络和信息系统的各种安全事件及行为实行监测、信息采集、分析并针对特定事件及行为采取相应的比较动作，并通过评估网络和信息系统的安全性和风险，为完善安全策略的制定提供审计数据和审计服务支撑，从而达到保障网络和信息系统正常运行的目的。

企业网络与信息系统安全事件审计产品是对网络和信息系统各组成要素进行安全事件采集，将采集数据进行自动智能分析，从而提高企业网络和信息系统安全管理的效率。

8.4.1　概述

安全事件审计主要是指企业监控并记录网络和业务系统环境中发生的安全事件，通过对各类安全事件审计日志信息的采集、分析、统计、呈现，以及对安全事件的发生、响应处理进行追踪，以及对后续的安全运维和安全策略进行完善改进。企业安全事件审计的目的是要全面掌控安全事件的状况，并查找在安全事件发生、响应处理等过程中是否存在问题，并及时督促完善，指导企业建立和完善信息安全运维体系。

企业为提高安全事件审计信息处理的准确性、真实性和合法性，强化企业的内部信息安全控制制度的落实，防止企业网络和业务系统出现各种安全隐患，应建立企业网络和业务系统环境下对安全事件审计的制度。内部安全事件审计是需要由企业的最高负责人直接领导下，依照有关信息安全法律、法规及内部信息安全管理制度，对安全事件真实性、完整性和时效性进行相对独立的监控、检查与评价的活动。其主要目的是保护企业安全事件审计信息记录的真实性与可靠性。

8.4.2　面临挑战与需求分析

随着企业对信息安全重视程度的增加，针对企业网络和业务系统发生的各类安全事件审计也越来越受关注，许多的安全厂商也随之提供许多相关的安全产品。企业通过查看、分析各类安全事件，定位与解决所发生的安全问题。但是随着时间流逝，企业面临更多安全事件审计需求，当前企业更加关注的审计需求有以下几个方面：

（1）如何保障安全事件审计信息的完整性、不可更改性，企业在对安全事件进行审计时，安全事件审计信息数据的完整性、不可变更性至关重要。

（2）企业每天产生海量安全事件审计信息，并且由于信息安全建设的异构化，各类安全厂商的安全事件审计信息格式不统一，如何统一进行安全事件审计信息的采集，统一管理，统一存储。

（3）企业该如何发掘安全事件审计信息中的价值数据，如何进行智能化分析、统计、呈现，从而更好地指导企业信息安全管理以及安全策略的制定。

8.4.3 安全事件审计的具体工作

安全事件审计标准流程是安全事件审计工作的具体规程，它规定安全事件审计工作的具体内容、具体的方法和手段。与安全审计一样，安全事件审计主要包括三个阶段：审计准备阶段、实施阶段以及终结阶段。

1. 安全事件审计准备阶段

安全事件审计准备阶段需要了解审计各类安全事件的具体情况、目标，以及安全事件响应控制措施和应用控制情况，并对安全事件审计工作制定出具体的工作计划。在这一阶段，应重点确定审计对象的安全要求、审计重点、可能的漏洞及减少漏洞的各种控制措施。

2. 安全事件审计实施阶段

安全事件审计实施阶段的主要任务是对企业现有的安全事件进行采集、分析、统计与呈现，以及如何快速进行安全事件响应、处理，从而明确企业是否为安全采取了适当的控制措施，这些控制措施是否发挥着作用，以及控制措施是否需要完善改进。

3. 安全事件审计终结阶段

安全事件审计终结阶段应对企业现存的安全事件采集、分析、统计、呈现平台系统作出评价，并提出改进和完善的方法和其他意见，特别是对企业信息安全运维体系建设、安全策略制定等等。

8.5 安全外包服务

外包服务是指企业将 IT 系统开发、架构、应用管理、业务流程优化等等自身业务需求通过外包给专业 IT 厂商来完成。企业信息安全外包服务（Information Security Outsourcing Service），是指企业将全部或者部分信息安全工作指定专业安全厂商来完成的服务模式。企业因自身需要考虑，或者需要更多关注自身核心业务，而企业信息安全不是其专注的内容，故此需要将企业信息安全工作交由专业安全厂商来完成。其不同于企业 IT 外包服务，将由企业内部部门和人员所要承担的 IT 系统，以及相关所有业务流程的运营、维护，支持的 IT 服务都由外部专业厂家来完成。

8.5.1　概述

企业信息安全并不直接推动业务发展，但与业务发展息息相关，由于信息安全管理工作的复杂性，造成企业对安全管理常常是“有心无力”，或者付出了代价，却不能获得相应的回报。而且对于现代企业来讲，信息安全工作内容是复杂的、繁重的，企业应该从中解脱出来，集中精力处理、开拓或发展业务。

企业安全外包服务的内容非常广泛，广义上讲，安全厂商为企业客户提供的各类安全产品维护服务、专业咨询服务、培训服务等等都在其中；从定义的角度讲，为企业提供信息安全外包服务是全面、专业、高效、安全地管理企业的安全设备，处理安全问题，保证客户业务价值的实现。

企业信息安全外包服务的风险是必然存在的，如何掌控风险，首先要了解存在的风险主要有哪些？首要就是信任风险，企业能否与信息安全服务的外包商建立良好的工作和信任关系，是决定将信息安全服务外包的重要因素；其次是依赖风险，信息安全服务外包使得企业很容易对服务厂商产生依赖性，并且受其商业的变化而受到制约；再有就是所有权风险、共享环境风险、实施过程风险等。这些风险的存在，都使得企业信息安全服务外包必须要有一个系统化管理模式。

8.5.2　需求分析

信息安全是动态的，是永远无法一劳永逸的，企业通过已有的信息安全管理体系保障企业自身信息安全避免损失是完全可能的，然而企业受限于自身信息安全管理能力与水平，甚至是企业组织结构与文化，对于十分专业的信息安全工作无法承担，往往需要专业安全厂商提供必要协助，根据企业客户具体情况和要求，安全外包服务的具体需求也各不相同。

信息安全合规审核评估服务是当前企业安全外包服务最迫切的需求之一，它是由信息安全厂商提供资深、专业的咨询师，基于企业法规、标准与策略遵从需要，在企业客户的组织体系、管理制度、业务系统，甚至操作系统的基础之上，帮助企业建立量化评估体系，为企业提供最真实、专业、全面的信息安全评估报告。企业的安全外包服务需要还有很多，如信息安全咨询与培训服务，企业网站安全检测服务，企业病毒防护清除服务，企业安全评估与加固服务，定制化、集成化的信息安全外包服务等。

8.5.3　安全服务外包的工作

1. 企业服务外包的策略与管理

企业若想做好信息安全外包服务活动，就需要建立一个完善的管理框架，如此企业才能实施和管理外包活动，协调与外包服务商的关系，最大限度地降

低信息安全外包服务的风险，从而达成实现企业业务价值的目标。

（1）信息安全政策制定

企业首先需要制定完善的信息安全策略，指导企业如何对资产以及敏感信息进行管理、保护，需要明确企业对信息安全目标、原则、标准和责任进行简要说明。选择适合企业信息安全管理的法规标准，目前企业通用的信息安全管理标准有两个，即信息安全管理体系标准 BS 7799 和信息安全管理标准 ISO 27001。

（2）明确信息安全外包服务的流程

根据企业的商业特点，以及信息安全外包服务的需求、范围，制定符合企业特点的信息安全外包服务流程。

（3）制定信息安全外包服务的管理原则和优化措施

制定信息安全外包服务的管理原则和优化措施主要是阐明企业信息安全外包服务要如何运作执行，执行的通用标准和尺度，明确服务外包商的任务和职责。信息安全外包服务是一个持续的工作，需要不断地采用各种优化措施进行完善。

（4）服务外包商的管理

企业需要管理好与外包商之间的关系，特别是可以长期合作的服务外包商，与之建立长期的合作伙伴关系或者战略同盟，企业在管理服务外包商时，在注重监督和控制的同时，还需要适当地进行协同与激励。

2．企业安全服务外包的基本内容

1）技术人员值守

企业现场技术人员值守服务，保证网络的实时连通和可用，保障接入交换机、汇聚交换机和核心交换机的正常运转。现场值守的技术人员每天记录网络交换机的端口是否可以正常使用，网络的转发和路由是否正常进行，进行交换机的性能检测，进行整体网络性能评估，针对网络的利用率进行优化并提出网络扩容和优化的建议。

现场值守人员还进行安全设备日常运行状态的监控，对各种安全设备的日志进行检查，对重点事件进行记录，对安全事件的产生原因进行判断和解决，及时发现问题，防患于未然。

同时能够对设备的运行数据进行记录，形成报表进行统计分析，便于进行网络系统的分析和故障的提前预知。具体记录的数据包括配置数据、性能数据和故障数据。

2）现场巡检服务

现场巡检服务是对企业的设备及网络进行全面检查的服务项目，通过该服务可使企业获得设备运行的第一手资料，最大可能地发现存在的隐患，保障设备稳定运行。同时，有针对性地提出预警及解决建议，使企业能够提早预防，最大限度降低运营风险。巡检内容一般包括硬件运行状态检查、软件运行检查和网络整体情况运行检查。

3）网络运行分析与管理服务

网络运行分析与管理服务是工程师通过对网络运行状况、网络问题进行周期性检查及分析后，为企业提出指导性建议的一种综合性服务，其内容包括专家支持、电话回访、分析报告等。

4）重要时期专人值守服务

对于企业来讲，在业务运行的重要时期，设备稳定运行对客户尤为关键。重要时期主要包括政府客户的重大会议期间、金融客户的年终结算日、运营商客户的生产网络重要组配期间或其他任何客户认为可能对其业务运营产生重大影响的时刻。

第9章

信息安全技术体系

信息安全技术体系同信息安全管理、信息安全运维体系一样是信息安全架构的重要组成部分。安全技术体系是安全运维和管理的对象，其功能由各自的子系统提供保证。本章从企业信息安全技术体系的构架、设计、实施等诸方面，描述了构建企业信息安全技术体系需要迎接的主要挑战，给出了企业信息安全技术体系，特别是数据保护体系的系统设计、实施部署。本章从以下几个方面对企业信息安全技术体系的建设展开论述：

（1）物理安全；
（2）网络安全；
（3）主机系统安全；
（4）应用安全；
（5）数据安全；
（6）灾难备份与恢复；
（7）内容安全；
（8）终端安全。

9.1　概述

评估信息系统是否安全实施，数据保护是否达到设计目标，其涉及的因素是多方面的。它涉及技术方面（如信息系统接入、操作系统、应用软件、数据防止非法入侵、软件绿色度认证等）、非技术方面（人员素质培养，管理监管制度建立，建筑、设备电器安全等）等多种因素。本节阐述我们在信息系统安全实施设计中的一些研究和体会。

9.1.1　问题与方法论

企业的信息安全建设可以通过特定安全问题与支撑的安全技术两个方面展开实现，企业信息化建设需要基于当前通用的网络与信息安全基础技术，从而使得信息化建设与安全技术有一个共同的基础。从安全问题角度讲，企业需要

对信息化建设与信息安全建设进行分析与总结，包括建设现状与发展趋势的完整性分析，归纳当前存在和今后可能存在的安全问题，明确网络与信息系统运营所面临的安全风险级别。从安全技术角度讲，企业需要从现有网络与信息技术的已有缺陷出发，总结普遍存在的安全危险，依托信息安全建设实践经验，从信息安全领域的完整框架、思路、技术与理念出发，提供完善的信息安全建设思路与方法。

以信息安全管理总体策略为核心，分三个方面进行整体信息安全体系框架的制定，包括信息安全技术体系、信息安全管理体系与运营保障体系。在企业实际运营过程中，信息安全管理体系不能够纯粹依靠信息安全技术体系来解决，更需要适当的安全管理互相协同来提高整体防御能力。

9.1.2　需要考虑的原则

从理论上讲，虽然不可能建立绝对安全和保密的企业信息安全技术体系解决方案，但如果在建设之初就遵从一些合理的原则，那么相应的安全性和保密性会得到大大提升。从工程技术角度出发，在设计信息系统安全方案时，应该遵循以下原则：

（1）安全与保密的“木桶原则”。我们需考虑对信息系统数据信息均衡、全面地进行安全保护。“木桶的最大容积取决于最短的一块木板”，攻击者使用的是“最易渗透原则”，必然会在系统中最薄弱的地方实施攻击。

（2）信息系统安全方案的“整体性原则”。综合考虑安全防护、监测和应急恢复信息系统安全方案应该包括三种机制，即安全防护机制、安全监测机制和安全恢复机制。

（3）信息系统安全方案的“有效性与实用性”原则，不能影响系统的正常运行和合法用户的操作。如何在确保安全性的基础上，把安全处理的运算量减小或分摊，减少用户记忆、存储工作和安全服务器的存储量、计算量，应该是一个信息安全设计者主要解决的问题。

（4）信息系统安全方案的“安全性评价”原则。 除了并不实用的一次一密码体制，所有的密码算法在理论上都是不安全的。因此，评价信息系统安全方案是否安全，没有绝对的评判标准和衡量指标，只能决定于系统的用户需求和具体的应用环境。

（5）信息系统安全方案的“等级性”原则，区分安全层次和安全级别。良好的信息系统安全方案是分为不同级别的，包括对信息保密程度分级（绝密、机密、秘密、普密）、对用户操作权限分级（面向个人、面向群组、面向公众等）、对信息系统安全程度分级（安全子网、安全区域）、对系统实现结构的分级（应用层、数据系统层、链路层）等，从而针对不同级别的安全对象，提供全面的、可选的安全算法和机制，以满足信息系统中不同层次的实际需求。

（6）信息系统安全方案的“动态化”原则。整个系统尽可能引入更多的可

变因素，并具有良好的扩展性。所谓的“安全”也只是相对的和暂时的，不存在一劳永逸的信息系统安全方案，应该根据攻击手段的发展进行相应的更新和升级。

（7）设计为本原则，安全与保密系统的设计应与信息系统设计相结合。由于安全与保密问题是一个相当复杂的问题，因此必须群策群力搞好设计，才能保证安全性。

（8）自主和可控性原则。信息系统安全与保密问题关系着一个国家的主权和安全，所以信息系统安全产品不可能完全依赖于从国外进口，必须解决信息系统安全产品的自主权和自控权问题，尽量采用有自主产权的安全产品。同时为了防止安全技术被不正当使用，必须采取相应的控制措施，如密钥托管技术等。

（9）权限分割、互相制约、最小化原则。对系统超级用户权限加以限制，按权限最小化原则分配权限，并使管理权限交叉，由多个管理用户来动态地控制系统的管理，实现互相制约。而对于非管理用户即普通用户，则按权限最小原则，不允许其进行非授权以外的操作。

（10）有的放矢、各取所需原则。安全无价，但是信息系统的建设是受经费限制的。因此在考虑安全问题解决方案时必须考虑性能价格的平衡，而且不同的信息系统所要求的安全侧重点各不相同。

以上设计原则可以在一定程度上为信息系统安全方案的设计提供参考。随着技术的进步和社会的发展，各种新的设计原则还将会层出不穷，应注意随时吸纳。以下对主要的信息系统安全措施予以分析探讨。

9.2 物理安全

物理安全是安全体系架构的技术和基础，有一个达到安全保障要求的安全物理网络和物理技术体系结构，是我们要解决的基本问题。

9.2.1 安全措施之物理隔离

通常使用的防火墙设备是为信息系统出入结点所设计的，是最主要的信息系统监控和安全设备，但类似的常规性信息系统安全防护产品已不能满足某些重要或敏感信息了，包括电力实时信息系统的信息保密需求。为保证这些重要信息在处理、传输和存储过程中的安全保密性，目前所能采取的最好的解决方法，就是建立一个与外部完全隔绝的内部信息系统。

具体物理隔离的技术实施方法简要描述如下：

第一代物理隔离技术：将两台计算机合并到一个机箱中使用，这种采用两套主板、芯片、网卡和硬盘的系统，只是节约了用户一个电源和显示器的投资而已。

第二代物理隔离技术：以双硬盘隔离和信息系统隔离技术为主，采用两个硬盘各自安装一个操作系统，在内、外不同的系统环境中独立启动一个硬盘，以达到单机分离接入不同系统的目的。

第三代物理隔离技术：其工作原理是，通过对单个硬盘上磁道的读写控制技术，在一个硬盘上分隔出两个工作区间，这两个区间无法互相访问。同时单硬盘物理隔离卡可提供一个第三分区，通过读写技术允许数据从外网分区向内网分区单向流动，方便了用户从互联网上下载数据。单硬盘物理隔离卡能在不增加其他任何硬件和软件成本、不用对系统重新设置的情况下，实现单台计算机连接内外两个系统，替代用独立的两套计算机信息系统实施的物理隔离方案，完全杜绝了各种可能的内部及外部信息系统的攻击或泄密的情况。即使是软盘及调制解调器这类通常无法控制的接入方式，都可以处于信息系统管理员的严格监控之下。而且，不同系统环境下的信息可以在信息系统管理人员的监控下进行交换，解决了物理隔离之后某些信息无法安全地进行交换处理的问题。

9.2.2　环境安全

1．机房与设施安全

企业信息系统的安全性、可靠性，首先需要对信息系统实体有一个安全的环境条件，通常指的是机房及其基础设施，以及保证企业业务系统正常工作的基本环境，如机房的建筑结构、选址、室内装修等。对机房与基础设施的安全保护，在 GB 50174－2008《电子信息系统机房设计规范》、GA/T 390—2002《计算机信息系统安全等级保护通用技术要求》、GB/T2887－2011《计算机场地通用规范》、GB/T9361－2011《计算机场地安全要求》等标准中有详细的描述。

2．环境与人员安全

环境与人员安全通常是指防火、防水、防震、防振动冲击、防电源掉电、防温度湿度冲击、防盗以及防物理、化学和生物灾害等，是针对环境的物理灾害和人为蓄意破坏而采取的安全措施和对策。

3．其他自然灾害

针对其他自然灾害的防护措施，主要包括湿度、洁净度、腐蚀、虫害、振动与冲击、噪声、电磁干扰、地震、雷击等。

9.2.3　设备安全

设备安全主要包括计算机设备的防盗、防毁、防电磁泄漏发射、抗电磁干扰及电源保护等。

1．防盗和防毁

当计算机系统或设备被盗、被毁时，除了设备本身丢失或毁损带来的损失外，更多的损失则是失去了有价值的程序和数据。因此，防盗、防毁是计算机防护的一个重要内容。通常采取的防盗、防毁措施主要有：设置报警器、锁定装置、计算机保险、列出清单或绘出位置图等等。

2．防止电磁泄漏发射

抑制计算机中信息泄露的技术途径有两种：一是电子隐蔽技术，二是物理抑制技术。电子隐蔽技术主要是用干扰、调频等技术来掩饰计算机的工作状态和保护信息；物理抑制技术则是抑制一切有用信息的外泄。

3．防电磁干扰

电磁干扰是指当电子设备辐射出的能量超过一定程度时，就会干扰设备本身以及周围的其他电子设备的现象。计算机与各种电子设备和广播、电视、雷达等无线设备及电子仪器等都会发出电磁干扰信号，计算机要在这样复杂的电磁干扰环境中工作，其可靠性、稳定性和安全性将受到严重影响。

另外，还需要特别提及的是介质安全，介质安全包括介质媒体本身的安全，以及介质媒体数据的安全。对媒体本身的安全保护是指防盗、防毁、防霉等；对媒体数据的安全保护是指防止记录的信息被非法窃取、篡改、破坏或使用。

9.3 网络安全

我国大中型企业网络平台的可靠性主要是通过物理层和链路层的安全来加以保证的。网络和计算机设备、通信线路以及业务数据的物理安全是企业安全的前提。尤其是要保护核心路由交换机及其他配套设施免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏。

9.3.1 网络安全设计

1．路由认证安全设计

为了防止非法入侵者将不正确的路由信息注入到企业网络的核心路由器或汇聚结点路由器的路由表中，网络中配置相邻认证路由的办法防止路由器或路由交换机接收欺骗性的路由更新，如图 9-1 所示。

在配置了“邻居路由认证”以后，只要路由更新在相邻路由器或路由交换机上交换，邻居认证就会发生。这种认证保证了企业网络中的关键路由器或交

换机接收到的均是可靠来源的路由信息。如果没有邻居认证，没有认证的恶意路由更新可能会使企业的网络通信安全性遭到伤害。例如，一个由非法入侵者控制的、未经认证的路由器可能会发送虚假的路由更新，使企业网络中的路由器信以为真，把 IP 包发送到不正确的目的地。这种误转目的地可以使别人能得到企业网络中的某些机密信息，或者破坏企业网络进行有效通信的能力。“邻居路由认证”可有效防止企业网络的关键路由器或路由交换机收到任何虚假的路由更新信息。

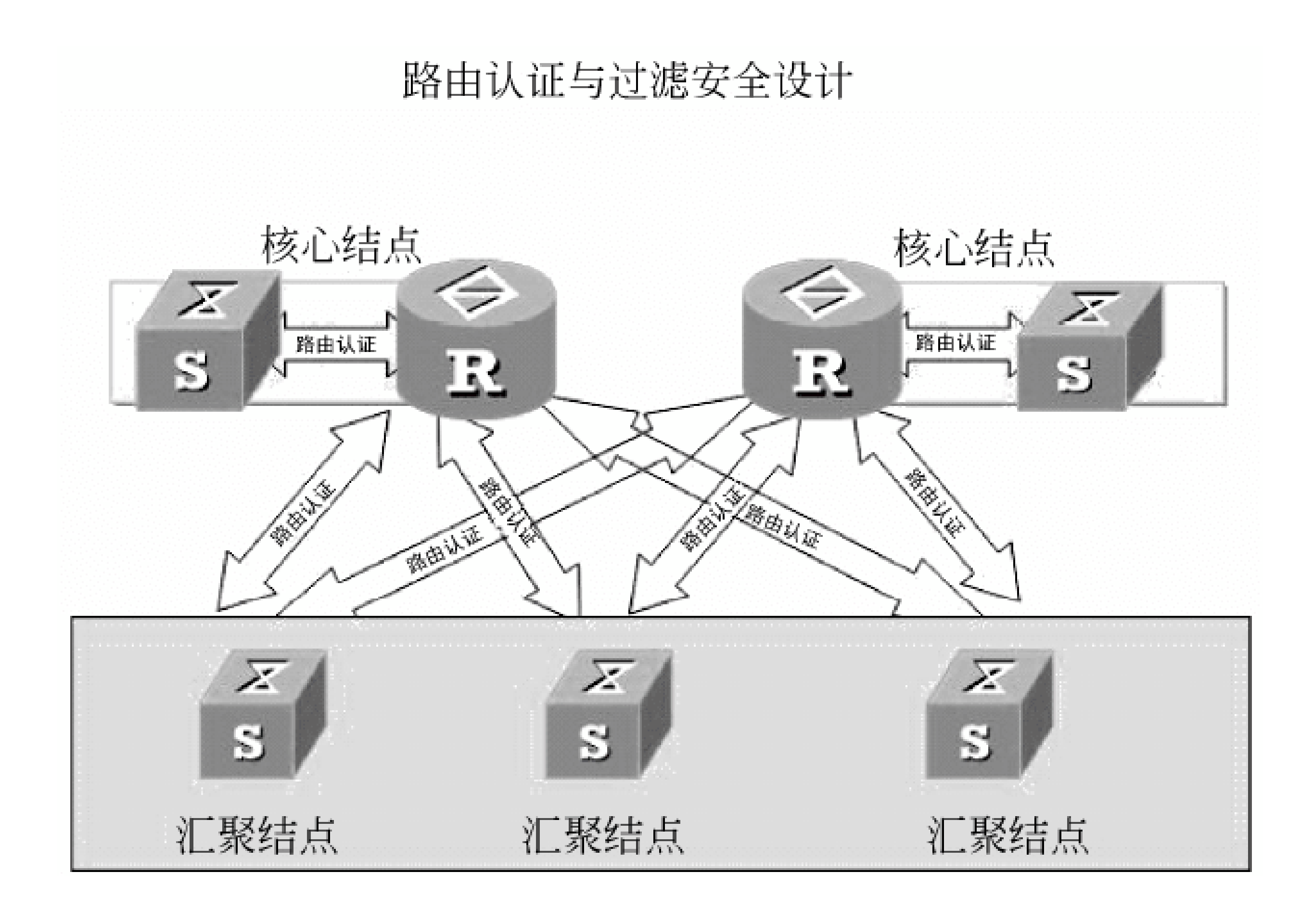


图 9-1　路由认证与过滤安全设计

当在路由器上配置了邻居认证以后，路由器或路由交换机将会检查它收到的每个路由更新包的来源。这是由交换发送和接收路由器都能识别的认证密匙（大部分时候是指一个密码）来实现的。可以使用两种邻居认证方法：纯文本认证和消息摘要算法版本 5(MD5)认证。两种方法都以相同的方式工作，但 MD5 发送一个“消息摘要”代替了认证密匙本身。这个消息摘要是由密匙和一个消息构成的，但密匙本身并不发送，这样可以防止在传送的时候泄露。纯文本认证则在线路上发送认证密匙本身。

2．网络综合访问认证设计

新型公司综合访问管理服务器（Comprehensive Access Management Server，CAMS）作为网络中的业务管理核心，支持与路由器、以太网交换机等网络产品共同组网，完成对终端用户的认证、授权、计费和权限管理，实现企业网络业务和用户的精细化可管理，保证网络和用户信息的安全，作为端点准入防御（EAD）的核心部件。

CAMS 系统提供下列特性：

（1）CAMS 采用 PC 服务器+Linux 的软硬件平台，数据库采用 Oracle。

（2）采用“平台+业务组件”的体系结构，基于 CAMS 平台之上，认证、计费等各业务模块相对独立。增加新业务时，平台无需改动，只需修改配置文

件，动态加载相应的业务组件。

（3）支持多业务、多协议统一认证。支持 Radius、Raduis＋协议，通过配置可以实现 PPPOE、802.1x、Web 等多种方式的认证，支持宽带接入业务。

（4）记录用户上网日志，日志记录中可以提供针对一次上网过程的用户名、源 IP 地址、上网时间段等信息，不能提供上网过程中所访问的目的 IP 地址信息。

（5）可通过内置 DHCP Server 功能，基于用户通过 DHCP 协议分配固定 IP 地址。

（6）支持与 LDAP Server 接口。

设计可以考虑企业在网管中心布署一台 CAMS 对局域网内的接入用户采用 AAA 认证和安全认证，同时实现网络访问权限的动态下发以及 Telnet 等权限。

在路由器和局域网交换机、CAMS 上进行详细的配置，只有来自特定网段的 Telnet 请求经认证后才能登录到该设备；同时，对登录的相关信息进行审计。

通过 CAMS 配合局域网接入层的智能三层交换机完成多种用户认证及访问权限控制手段，记录用户的上网行为，对上网者进行监控。实现网络接入层面的安全，将由人为主动行为或被动行为造成的网络安全隐患对网络带来的影响全面封锁在网络之外，充分保障网络的安全性、健壮性。

3. 入侵检测和漏洞扫描安全设计

入侵检测是安全网关的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是安全网关之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

企业在入侵检测和漏洞扫描安全设计方面的安全布署主要包括以下方面：

（1）在总部布署多套基于网络的入侵检测系统，使得网络具备对内外黑客非法网络入侵行为的实时检测和实时响应能力，确保在系统遭受破坏之前得以消除网络安全方面的威胁。

（2）在总部网络中布署一套基于网络的漏洞扫描系统，用来满足整个网络中的网络安全漏洞扫描能力和修复能力，堵塞住网络系统的安全漏洞。

（3）在总部布署一套基于主机的漏洞扫描系统，用来扫描网络中重要服务器（如计费服务器、认证服务器、网管工作站等）的安全漏洞，消除主机安全隐患。

9.3.2 网络设备安全特性

由于很多网络设备操作系统中内建的服务存在或多或少的安全漏洞，对于企业并不需要的功能，建议在网络实施过程中将这些特性设置为关闭，除非有

很明显的需要，否则不要打开它们。

同时，网络设备的安全配置主要考虑下列安全特性：

（1）采用 802.1x 方式对接入用户进行认证，支持安全的 SNMP v3 的网管协议、支持配置安全，对登录用户进行认证，不同级别的用户有不同的配置权限，并提供两种用户认证方式：本地认证和 RADIUS 认证。

（2）端口绑定功能：支持 MAC、IP、VLAN、PORT 任意组合绑定，有效地防止非法用户访问网络。支持多种 ACL 访问控制策略，能够对用户访问网络资源的权限进行设置，保证网络的受控访问。

（3）VLAN 部署如下：

① 支持丰富的统计信息包括各种流量的统计、流采样、NAT 信息统计。

② 支持策略路由、NAT 安全日志、端口镜像。

③ 端口安全性设定。利用交换机的端口与 MAC 地址绑定功能将企业网络中一些重要服务器和工作站（如计费服务器、认证服务器、网管工作站等）的 MAC 地址和局域网交换机的交换端口相绑定，从而杜绝内部网中假冒服务器 IP 地址的非法攻击行为。

9.3.3 路由安全

伴随着信息技术的飞速发展和企业信息化程度的不断提高，多业务融合的宽带网络已经成为企业正常运营的重要保障。为了确保一个稳定、安全、高效的网络运营环境，管理员不得不常常面临以下问题：如何监控用户的网络应用行为？如何跟踪网络应用资源的使用情况？如何识别网络中的异常流量和性能瓶颈？如何有效地规划和部署网络资源？

上述问题归结的一点，就是实现路由安全。

1. 采用 XLog 系统

这些问题的解决依赖于管理员对网络运行详细状况的及时获取，为此，建议采用新型网络日志审计系统（Network Log Audit System，XLog），可以与路由器、交换机、BAS 等网络设备共同组网，根据用户要求采集不同类型的网络流量信息，并通过聚合、分析与统计，为网络管理员提供用户行为审计、流量异常监控和网络部署优化的数据基础和决策依据。

具体的部署为：在企业网络部署两台服务器，一台是 DIG 采集服务器，另一台是 XLog 服务器，共有两个网络位置需要探测日志，在局域网内部，在 8508 上做端口镜像，将需要审计的数据镜像到 DIG 采集服务器，用探针的方式采集日志后将日志传送到 XLog 服务器进行分析。

因为 IDS 的安全联动也需要使用镜像端口，这时可能遇到镜像端口不够用的情况，可考虑使用 TAP 设备，TAP 设备相当于有线电视上的分流器，即将一份流量复制成两份。

XLog 可根据用户需要，通过各种组合条件对海量的网络日志进行快速分析，如图 9-2 所示。管理员可以从日志审计结果中准确了解终端用户的上网行为——用户何时访问了某网站？何时访问了某网页？发送了哪些 Email？向外传送了哪些文件等。

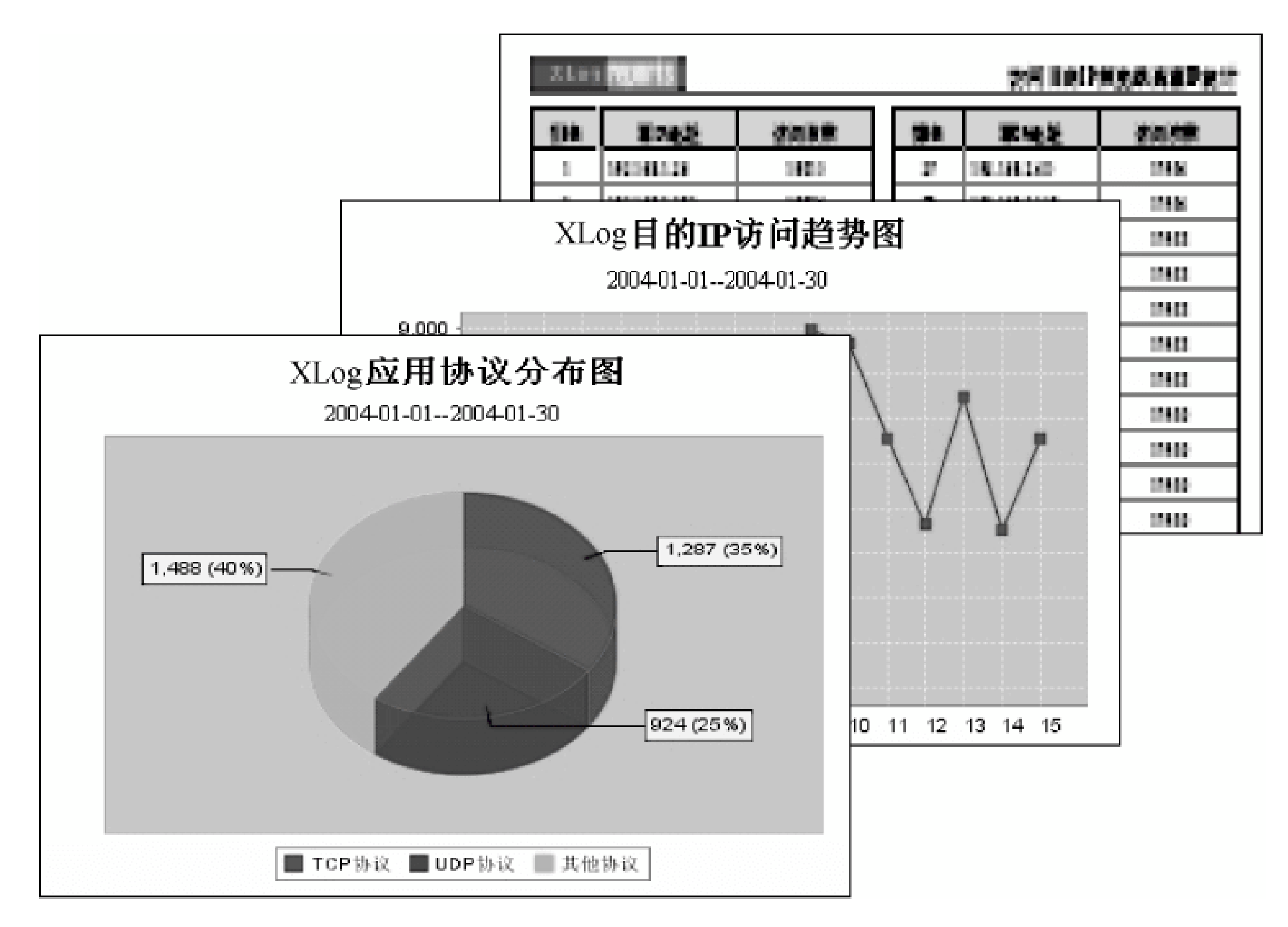


图 9-2 Xlog 示意图

2. 全网采用 SNMP v3 的网管

企业所用到的如果是全部新型网络设备，都支持 SNMP v3 的网管协议和 SSH（Secure Shell)，可以使网络管理员在管理设备时口令不被窃取，保证了网络管理权限的安全。

3. 结论

经过企业网络建设过程中涉及的网络平台、业务系统中存在和可能出现的问题的深入分析，集成商从网络层面及系统层面，从事前的防范到事中的监控，直到事后的审计，通过建立完善的安全机制、部署网络安全策略，对于设备物理安全、系统安全、业务安全及用户接入安全等方面给出了建设性的意见。

同时，这里要指出，网络的安全是全面协防的概念，而非仅依靠某一层次或某一设备予以解决。全面的安全协防旨在不同层次上利用不同技术、不同成本的设备相互补充，从而既加强了安全，又平衡了安全中存在的矛盾。

9.3.4 VPN 技术及其应用

1. VPN 技术概述

企业现在面临着不断开放企业的内网来处理各项内外业务，因此，如何建

立一个安全、高效、易用、经济的网络接入方式，保障企业的各项应用系统推广到企业以外使用就成为当前众多企业所面临的挑战。

早期，建立保密的网络连接一种方案是使用专线，如 SDH、MSTP 等。但是这种方式存在非常大的两个缺点：一是不灵活，不能满足出差人员随时随地接入的需求；二是费用高，专线方式的网络连接需要支付高昂的专线租用费用。

随着 VPN（虚拟专用网络）技术的发展，VPN 技术已经成为一种非常成熟的网络连接方式，可以有效支持企业通过 Internet 等公共互联网络与固定的局域网、个人终端等建立加密的数据连接，进行安全的通信，防止黑客嗅探到敏感的数据。这种跨越 Internet 建立的 VPN 连接逻辑上等同于两地之间使用广域网建立的连接，它具有高性价比、强适应能力、很强的网络安全特性以及动态的扩展能力等优势，已经广泛替代专线用来进行广域网络的衔接。VPN 技术的关键组成部分包括隧道技术、加密技术、身份认证等，在此我们就不再赘述了，大家可以参考一些专业的安全技术文献。

2. VPN 技术的分类

目前，区分 VPN 技术主要是根据其隧道协议的不同类进行的，下面将重点介绍 IPSec 和 SSL 两种最常用的 VPN 隧道技术。

1）IPSec 协议

IPSec 是 IETF 支持的标准之一，它是第三层即 IP 层的加密。IPSec 不是某种特殊的加密算法或认证算法，也没有在它的数据结构中指定某种特殊的加密算法或认证算法，它只是一个开放的结构，定义在 IP 数据包格式中，不同的加密算法都可以利用 IPSec 定义的体系结构在网络数据传输过程中实施。

IPSec 协议可以设置成在两种模式下运行：一种是隧道（tunnel）模式，另一种是传输（transport）模式。在隧道模式下，IPSec 把传输层的数据包封装在安全的 IP 包中。传输模式是为了保护端到端的安全性，即在这种模式下不会隐藏路由信息。隧道模式是最安全的，但会带来较大的系统开销。由于 IPSec 是基于网络层的，不能穿越通常的 NAT 及防火墙。

IPSec VPN 的部署方式为 Site to Site、Client to Site，即采用网关到网关、客户端到网关两种方式。除需要在总部部署 VPN 网关外，还需要在分支部署网关或者 PC 上部署客户端，并且配置加密方式、认证方式、密钥信息、算法、接入地址等复杂的设置。

此外，IPSec 协议在实现安全性的同时，网络传输效率有所下降。因此，作为国内的 VPN 行业标准制定者的深信服科技（Sangfor）提出了基于 IPSec 协议改进的 SANGFORSL 协议（ SANGFOR IPSec VPN 采用的安全链路协议），主要改进了以下两点：

（1）提供压缩的 IP 头算法，由此提高网络利用率。普通的 IPSec 网络利用率在 70%左右，而 SANGFORSL 可达到 90%。

（2）改进的 IP 封装技术，使得 SANGFORSL 可通过任何路由器，提高对网络的适应能力。

SANGFORSL 提供基于挑战－响应模式的身份认证，同时也提供基于硬件证书（HARDCA）的鉴权体系。数据传输采用隧道模式，支持各种加密算法，对会话的管理更具有灵活性，同时能适应各种网络层。目前，根据 IDC 等权威机构的调查显示，采用 SANGFORSL 协议的深信服 VPN 设备已经占到了 35%以上的市场份额。

2）SSL 协议

安全套接字层（Secure Socket Layer，SSL）属于高层安全机制，广泛应用于 Web 浏览器程序和 Web 服务器程序，提供对等的身份认证和应用数据的加密。在 SSL 中，身份认证是基于证书的。服务器方向客户方的认证是必须的，而 SSL 版本 3 中客户方向服务器方的认证只是可选项，并没有得到广泛的应用。SSL 会话中包含一个握手阶段，在这个阶段通信双方交换证书，生成会话密钥，协商以后通信使用的加密算法。完成了握手以后，应用程序就可以安全地传输数据而无需做很大修改，除了在传输数据时要调用 SSL API 而不是传统的套接字 API。

SSL VPN 工作于 SSL 协议的通信中，保证 PC 访问与所有代理服务器或 VPN 网关之间的畅通。一旦连接成功，一个小型的基于 Java 的客户端就会被下载到计算机的 Web 浏览器，会在您的计算机和 VPN 网关之间创建一个虚拟连接。

如果需要，Web SSL VPN 会自动下载至用户计算机，还可以自动安装。当终端用户会话结束后，这个连接也会自动从计算机上删除，清除 VPN 客户端的使用痕迹。这意味着，使用 SSL VPN 的客户端可以放心从其他计算机上登录公司网络，无需安装特殊的认证程序或其他加密系统。用户只需要知道他们自己的数字认证以及连接到 VPN 网关上的 URL 地址。

但是，目前 SSL VPN 技术主要是在移动办公环境下使用，大多采用 3G、WiFi 等接入方式，链路传输质量不高，延时高、丢包高等情况会极大地影响访问速度和用户体验。因此，如果能在 SSL VPN 安全特性的基础上增加一些网络优化技术（如 TCP 协议优化、流缓存、压缩等技术），就可以提升网络传输速度 200%以上，优化用户体验，提升满意度。建议企业用户在采用 SSL VPN 设备时关注其是否具备一定的网络优化技术。

3. VPN 技术的对比

在企业日常的 IT 建设过程中，大家经常会问的一个问题就是：SSL VPN 和 IPSec VPN 技术应该采用哪种更加合适，该如何选择？首先从表 9-1 中的性能对比来看二者的一些区别。

表 9-1　VPN 技术对比表

	工作层次	组网方式	接入方式	安全性	灵活性	易用性
IPSec VPN	网络层	Site to Site、Client to Site	硬件网关、客户端软件	控制粒度较粗	中等，需要部署网关、客户端	中等，配置负责
SSL VPN	应用层	Client to Site	Web 浏览器/零客户端配置	控制粒度更细	高，无需部署设备、客户端	强，零配置即可使用

由此可见：

（1）对于分支机构（有多台 PC 的局域网）与总部互联时，更适合 IPSec VPN 技术；

（2）对于出差员工移动接入、大量分散的合作伙伴/客户接入总部时，更适合采用 SSL VPN 技术。

4. VPN 技术的典型应用场景

1）远程移动接入访问

随着当前移动办公的日益增多，内部员工可以通过 SSL VPN 技术直接在 PC、各种移动终端上通过 WiFi、3G、有线、卫星等方式接入互联网与总部建立 VPN 访问企业的内部应用资源。远程移动接入访问主要针对的场景有：

（1）对于出差员工移动接入，访问 OA 系统等。

（2）移动营业网点的远程办公人员，进行移动销售、移动开户、移动执法、野外勘探等。

（3）微型办公室员工访问 OA、ERP、CRM 等系统。

（4）无需开发 APP，移动终端就可以采用应用虚拟化+SSL VPN 直接访问内部业务系统。

2）企业内部分支互联访问

企业采用 IPSec VPN 的方式可以通过 Internet 等公用网络进行企业各个分支机构的互联，是传统的专线网扩展或替代形式。企业内部分支互联访问的主要使用场景如下：

（1）各种大中小型分支通过 IPSec VPN 网关与总部互联。

（2）为了提升分支与总部之间线路的可靠性，除了专线外，分支可以增加一条 VPN 线路作为备份链路。

（3）对企业网络内部的某些关键应用系统（比如财务等），需要与企业应用隔离，防止数据泄密时，可以在原有的专线上构建 VPN 方式来实现（IPSec VPN 和 SSL VPN 都可以考虑）。

3）企业外部合作伙伴互联

企业外部合作伙伴互联是指利用 SSL VPN 将企业的应用系统延伸至合作伙伴与客户。大家都知道，合作伙伴和客户数量较多，也相对分布分散，采用专线接入成本较高、管理复杂。因此，在以下场景——第三方合作伙伴接入，如企业的经销商通过 ERP 订货、运营商的合作营业厅访问 BOSS 系统、统计局“企业一套表系统”收集信息等——采用 SSL VPN 技术尤为常见。

9.3.5 网络威胁检测与防护

面对网络应用层威胁，目前业界主要是通过深度包检测（DPI）、Web 应用代理等技术深入到 IP 报文应用层和内容进行分析，与已知的各种应用威胁特征

进行比对后，拦截各种应用层威胁的方法进行防护的。目前，我们常见的应用层安全防护技术和设备主要分为以下几种：

1. IDS（入侵检测系统）

IDS 是英文“Intrusion Detection Systems”的缩写，中文意思是“入侵检测系统”。专业上讲就是通过 DPI 技术，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

形象的比喻就是：如果说防火墙是一幢大厦的大门，那么 IDS 就是这幢大厦里的视频监控系统。一旦小偷或内部人员有非法行为，只有实时监视系统才能发现情况并发出警告。

与防火墙不同的是，IDS 是一个旁路监听设备，没有也不需要跨接在任何链路上，无须网络流量流经它便可以工作。因此，对 IDS 部署的唯一要求是：IDS 应当挂接在所有所关注的流量都必须流经的链路上。

IDS 在交换式网络中的位置一般选择为：尽可能靠近攻击源、尽可能靠近受保护资源。这些位置通常是：服务器区域的交换机上、Internet 接入路由器之后的第一台交换机上、重点保护网段的局域网交换机上等。

但是 IDS 也存在一定的问题：

（1）针对单包类型的攻击，可以直接穿透 IDS，即使 IDS 与防火墙形成了联动也无法防护。

（2）IDS 的漏报、误报较多，让 IT 管理人员在海量的信息中无法及时、准确地获取有价值信息。

因此，大家通常对于 IDS 的定位是：IDS 重在全面检测，追求有效呈现，主要通过统计数据分析、多维报表呈现等管理特性，更加直观地让用户了解入侵威胁状况和趋势，以便支撑治理入侵的补充依据。

2. IPS（入侵防御系统）

IPS 是英文“Intrusion Prevention System”的缩写，中文意思是“入侵防御系统”。正是由于上述传统防火墙加传统 IDS 技术的一些弊端，如无法实时过滤一些新型的应用威胁，IPS 应运而生，简单的理解就是对流经的每个报文进行深度检测（协议分析跟踪、特征匹配、流量统计分析等），具备了实时、在线部署的能力，可以对恶意报文、攻击报文、病毒木马文件等进行丢弃，以阻断攻击等多种处理方式，如向管理中心告警、丢弃该报文、切断此次应用会话、切断此次 TCP 连接。

由此可见，在企业网络中，至少需要在以下区域部署 IPS，即办公网与外部网络的连接部位（入口/出口）、DMZ 的 Web 服务器前端、内网重要服务器集群前端、办公网内部接入层等。

但是由于 IPS 主要防护的对象是各种系统漏洞、病毒木马、一些简单的 SQL

注入等攻击，对于 OWASP Top10 的 Web 安全威胁缺乏有效的防护。对于内外网中一些关键 Web 服务器，仅仅部署 IPS 是不足够。

3. WAF（Web 应用防火墙）

WAF 是英文“Web Application Firewall”的简称，中文意思是“Web 应用防火墙”，它是通过执行一系列如 HTTP/HTTPS 代理等技术，制定一定的安全策略来专门为 Web 应用提供保护的一款产品。

与传统 L2-L4 防火墙、基于 DPI 技术的 IPS 相比，WAF 则是工作在 TCP/IP 第七层处理 HTTP/HTTPS 服务的，能够全面地识别各种 HTTP/HTTPS 数据包中的数据，从而有效地辨别出各种 Web 应用威胁、敏感数据内容，予以实时的拦截。比如可以提供以下更细致的安全策略：对协议的全面理解以及协议规范性检查；请求头关键字段的识别和特征匹配，从而降低误判；响应头敏感信息的处理防止服务器指纹泄露；响应体特征匹配，屏蔽敏感信息泄露。

因此，WAF 除了针对上文中提供的 OWASP Top10 的 Web 应用威胁提供防护过滤功能外，还可以针对 Web 应用中的敏感内容进行检测和拦截，从而防止客户信息等数据的泄露。

但是，WAF 产品的问题在于，防护的威胁范围仅限于 Web 应用，无法针对系统漏洞、网络设备漏洞、协议漏洞、Office/Flash 等应用漏洞进行防护。所以，WAF 在实际部署过程中需要与 IPS、FW 等产品一起配合使用。建议部署的位置是内外网重要的 Web 服务器前端，如门户网站、电子商务网站、网上营业厅等。

4. NGFW（下一代防火墙）

目前，黑客的攻击不再是以破坏为目的，更多的是试图窃取内部的机密信息，传统安全产品（防火墙、IPS、UTM）侧重于防护来自外部的已知攻击和入侵，对业务系统回复的信息内容不做检测，如果黑客利用未知漏洞进入网络窃取信息或篡改网页，这样的防护手段是没有作用的。但是单纯部署 WAF 设备防护类型有限。

因此，有些企业用户采用同时部署防火墙+IPS+WAF 方式来提高安全性，这种方式不仅成本很高，而且多台设备会产生更多的单点故障风险，还会导致网络性能下降。

那么如何在有效防护各种应用层安全威胁，提供双向内容检测过滤各种敏感信息的同时，尽量减少设备部署数量，提升可靠性、降低成本成为了很多企业用户的考虑重点。因此，下一代防火墙（Next-Generation Firewall）应运而生。

根据 Gartner 在 2009 年发布的一份名为《Defining the Next-Generation Firewall》的文章，给出了真正能够满足用户当前安全需求的下一代防火墙（NGFW）定义，结合当前安全发展趋势和一些主流 NGFW 产品的特点，笔者认为下一代防火墙需要满足以下几个方面的特点。

防应用层攻击：75% 的安全威胁源自应用层，下一代防火墙应该具备应用

层协议的识别能力，并能针对应用层安全威胁提供完整的解决方案。弥补传统安全设备由于工作在网络，只解析网络层数据包，无法理解应用层协议并防护应用层的安全威胁的问题。

双向内容检测：为了解决传统安全设备只针对外部攻击防护的问题，下一代防火墙应该具备双向的内容检测能力。除了能够防护外部攻击以外，需要对服务器响应的反馈内容进行严格的安全检查，以提供防网页篡改、防敏感信息泄露等功能。

涵盖传统安全：应用层的安全威胁日益盛行，但源自底层的网络层安全威胁仍然存在，其危害性也不容忽视。下一代防火墙应该涵盖传统防火墙、IPS、VPN 等功能，以减少多设备串行部署单点故障、性能瓶颈以及风险无法统一定位的问题。同时从用户长远利益考虑减少重复无效的投资，实现最优的投资回报。

应用层高性能：虽然多功能网关具备部分应用安全防护能力，但其传统安全设备的集成、串行部署的方式，使其在多种功能开启之后性能急剧下降，最终只能当传统防火墙使用。下一代防火墙应该从软件构架、硬件构架两方面彻底改变多功能网关由于多功能堆叠、串行部署导致的性能瓶颈问题，具备应用层高性能实现万兆的吞吐。

如果下一代防火墙能够真正实现上述的四类要求，它完全可以替代一些传统安全产品的部署场景部署在以下区域：互联网出口边界、内网各个安全域边界、内网重要服务器前端、外网 Web 服务器前端、广域网边界等。

目前，我们也看到 NGFW 的概念刚刚兴起，国外的代表厂商有 Paloalto 等，国内的代表厂商有深信服等。对于大多数客户来说，NGFW 有一个接受的过程，但是笔者认为 NGFW 正是由于其全面完整的安全防护功能、应用层的高性能以及一体化低成本的优势，将会成为下一个网络安全的建设重点，大量替换现有的传统 FW 等产品。

9.4 主机系统安全

主机系统安全也称操作系统安全，由于现代操作系统的代码庞大，从而不同程度上都存在一些安全漏洞。一些广泛应用的操作系统，如 UNIX、Window NT，其安全漏洞更是广为流传。另一方面，系统管理员或使用人员对复杂的操作系统和其自身的安全机制了解不够，配置不当也会造成安全隐患。

9.4.1 系统扫描技术

对操作系统层设备和系统的需要进行智能化的检测，以帮助网络管理员高效地完成定期检测和修复操作系统安全漏洞的工作。系统管理员要不断跟踪有关操作系统漏洞的发布，及时下载补丁来进行防范，同时要经常对关键数据和

文件进行备份和妥善保存，随时留意系统文件的变化。

9.4.2　系统实时入侵探测技术

为了加强主机的安全，还应采用基于操作系统的入侵探测技术。系统入侵探测技术监控主机的系统事件，从中检测出攻击的可疑特征，并给予响应和处理。

配置实时系统传感器对计算机主机操作系统进行自主地、实时地攻击检测与响应，一旦发现对主机的入侵，可以马上切断系统用户进程通信，作出各种安全反应。

实时系统传感器还具有伪装功能，可以将服务器不开放的端口进行伪装，进一步迷惑可能的入侵者，提高系统的防护时间。

9.5　应用安全

9.5.1　应用安全概述

应用安全的总体目标是保障其所实现的业务正常运行，防止应用系统遭受外部和内部的破坏和滥用，避免和降低对其所实现的业务系统的损害。应用系统是指根据业务要求设计开发的应用软件及其运行环境。

1．应用身份识别和认证

应用系统应提供除用户名/口令外其他身份验证机制，必要时还需支持双因素认证；同时还应具备登录控制模块，对用户身份鉴别信息复杂度检查、登录失败处理和用户身份唯一性标识等进行安全控制。

2. 访问权限控制

应用系统应实行独立的访问权限控制和基于角色的权限管理等功能，并对相关的资源进行细粒度的权限控制，从而最终通过安全标识的比较来确定主体对客体的访问是否合法。

3. 通信数据的机密性保护

应用系统应在通信过程中对其敏感信息，如客户账号、密码、交易金额等字段进行加密，同时保证其整个报文或会话过程也是加密的。

4．通信数据的完整性保护

应用系统应采用秘密的单向算法（如 MD5 等摘要算法）或事先约定的密码

用加密算法进行数据报文的完整性校验。常用的机制根据算法的类型可分为以下两种：

（1）数字签名：采用非对称加密机制，发送方利用自身的私有签名密钥计算报文的数字签名，接收方利用对方的公开签名密钥进行验证。

（2）报文验证码（MAC）：利用对称加密机制，在一定周期内，双方约定交易验证密码，发送方利用该密码计算交易验证码，接收方进行验证。

5. 密码管理

应用系统应对密码进行生命期的管理，并根据实际密级需求采用对应的对称加密和非对称加密的算法和密钥位数；如采用软件的密码管理系统，则应提供在系统安装初始化时产生密钥种子且其密钥种子不得固化在程序中的方法，同时如果密级较高时建议密码管理由相应的硬件完成，其密码装置还需具备防物理攻击的特性。

6. 可信路径

应用系统对用户进行身份鉴别时，应能够建立一条安全的信息传输路径；同时在用户通过应用系统对资源进行访问时，应用系统还应保证在被访问的资源与用户之间应能够建立一条安全的信息传输路径。

7. 通信保护

应用系统在其通信会话中应提供安全的标记方法和验证机制，必要时提供安全的密码保护技术，如专用的安全密码算法和硬件密码设备等。

8. 应用代码安全

应用系统应建立标准的代码编写安全规范，并严格要求开发人员进行执行，同时通过外聘专家对其静态代码进行扫描分析和应用的渗透性测试。

9. 应用安全审计

应用系统应提供完善的日志审计功能，能记录业务访问活动、账户管理活动、认证登录活动、配置管理活动和应用系统活动等类型的日志，并保证每类日志记录充分的信息内容，如时间、日志类型 ID、访问主客体名称、应用系统的操作类型、访问的资源名称等，同时能保证每类日志类型的格式唯一性和标准的日志输出接口，如 Syslog、Snmp trap 等。

10. 应用软件容错

应用系统应对输入数据进行有效性检验，包括用户通过人机接口输入或其他软件模块通过通信接口输入；通过专门的状态监控进程，当故障发生并中断退出时能向管理员提供故障类型和故障发生点的信息，同时保证在一般情况下

其他功能还能继续正常运行，即达到有限容错保护的目的；最后它还应提供自动恢复功能，当故障发生时立即自动启动新的进程，恢复原来的工作状态。

11. 应用软件资源配置

应用系统应支持将服务优先级的控制范围限定于某个资源子集，确定访问用户或请求进程的优先级，并指出对何种资源使用该优先级。如果一个访问用户或请求进程准备对由服务优先级控制的资源进行操作，那么其访问和/或访问时间将取决于其优先级、当前正在对该资源进行操作和等待进行该操作的队列中的访问用户或请求进程的优先级，达到有限服务优先级；同时提供其资源分配最大和最小的限额功能，能可确保某一访问用户或请求进程不会超过或低于某一数量或独占某种受控资源。应用软件可限定所要求的最大或最小资源分配限额的受控资源（如处理器、磁盘空间、内存、传输带宽）清单。

12. 应用安全保证

应用系统的安全保证是指从应用软件的设计、测试、分发、运行维护的过程来保证应用系统的安全性，防止由于管理不当引起的威胁，应用系统安全对应用安全保证的强度需求主要取决于由于管理不当引起风险的大小，具体包括版本和配置管理、测试、分发和操作等。

9.5.2 数据库安全

大多数业务系统都是运行在数据库平台上的，如果数据库安全无法保证，那么其上的应用系统也会被非法访问或破坏。

1. 主要数据库安全隐患

通过进一步的分析，数据库安全隐患的主要表现如下：

（1）系统认证问题：口令强度不够、过期账号、受到登录攻击等。

（2）系统授权：账号权限不清、登录时间超时等。

（3）系统完整性：特洛伊木马、审核配置、补丁和修正程序不及时等。

2. 解决方案——设置数据库扫描器

（1）配置方法：数据库扫描器（Database Scanner）可以与网络安全扫描工具安装在同一台笔记本式计算机上，也可以单独安装在一台 PC 上。定期对灾备中心内的数据库服务器软件进行漏洞评估，并将软件生成的漏洞报告诉分发给数据库管理员，对数据库系统中的安全问题及时修复。

（2）Database Scanner 漏洞检测的主要范围包括：

① 登录口令：口令长度、检查有登录权限的过去用户、检查用户名的信任度。

② 配置：是否具有潜在破坏力的功能被允许、配置是否需要修改。

③ 安装检查：打补丁及补丁的热链接。

④ 权限控制：一些用户有权限得到存储的过程及何时用户能未授权存取文件和数据资源。它还能检查“特洛伊木马”程序的存在。

⑤ 动态身份认证：数据中心重要主机和网络设备上要部署动态身份认证系统，实现中心各系统的主要网络设备、核心主机以及数据库的全网口令统一管理功能，更好地避免来自弱密码的威胁。

9.6 数据安全

数据安全通常有两方面的含义：一是数据本身的安全，主要是指采用现代密码算法对数据进行主动保护，如数据保密、数据完整性、双向身份认证等；二是数据防护的安全，主要是采用现代信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。

数据安全是一种主动的防护措施，必须依靠可靠、完整的安全体系与安全技术来实现。简单来讲，有关数据安全的内容可以简化为下列三个基本点：

1．机密性

机密性又称保密性，是指个人或团体的信息不为其他不应获得者获得。在现有信息系统中，许多软件包括邮件软件、网络浏览器等，都有保密性相关的设定，用以维护信息的保密性。在现实环境中，数据的机密性面临多种威胁，如间谍软件、黑客等，都可能造成保密性的问题。

2．完整性

数据完整性指在传输、存储信息或数据的过程中，确保信息或数据不被未授权的篡改或在篡改后能够被迅速发现。在实际的信息系统中，完整性常常和保密性边界混淆。比如，被加密后的数据在传输中被黑客或恶意用户破解，并通过一定的数学工具修改了密文中的有关数值或信息，数据接收者如果无法校对数据的完整性，将使用错误数据进行处理。为解决以上问题，通常使用数字签名或散列函数对密文进行保护。

3．可用性

数据可用性是一种以使用者为中心的设计概念，可用性设计的重点在于让产品的设计能够符合使用者的习惯与要求，也就是在确保数据机密性和完整性的同时，也要确保数据可以被使用者方便使用，而不能一味强调机密和完整忽视数据存在的根本意义是被使用和处理。

数据安全问题涉及数据整个生命周期的管理过程：从创建到失去商业价值或按规定要求被删除。就企业而言，所有的数据在其生命周期中都应当被有效的管理，通过必要控制手段清晰的界定，以使其避免内部非授权的访问。

9.6.1　数据危险分析

1. 安全风险综述

如今，企业机密信息大量以电子文档方式存在，而电子文档是很容易散播的。为此我们需要防止数据的泄密，在对付外部人员非法访问的时候，我们可以通过防火墙、入侵检测等防护系统进行防护，但是目前大量的信息泄密手段往往是最直接的收买、复制方式。这时，防火墙、入侵检测等防护系统就形同虚设了，根本起不到任何保护作用。因为防火墙或专网，只是解决了外部人员非法访问的问题，不能解决内部人员通过电子邮件、移动硬盘或笔记本式计算机把电子文档进行二次传播的问题。

据调查，企业机密泄露 30%～40%是由电子文件的泄露造成的。

（1）Fortune 排名前 1000 家的公司，每次电子文件泄露造成的损失平均是 50 万美元。

（2）对中国 500 家大型企业做的调查发现，国内的企业对电子文档几乎没有任何防护措施，有保护措施的不到 3%，一些机密性的资料、电子文档，轻易的就可以通过电子邮件和移动硬盘泄密到网络外部。

（3）在工业化时代，世界较大的商业秘密，代号 7X 的可口可乐配方，采取了严密的保护措施，为可口可乐公司赢得了超过 800 亿美元的无形资产的安全。

（4）中国千年绝活“景泰蓝”制瓷技术、“纸中之王”中国宣纸等技术被窃，为企业带来了难以估量的损失。

FBI 和 CSI 对 484 家公司调查，发现：

（1）超过 85%的安全威胁来自企业内部。

（2） 16%来自内部未授权的存取。

（3）14%专利信息被窃取。

（4）12%内部人员的财务被欺骗。

（5）11%资料或网络被破坏。

（6）防病毒、防火墙、入侵检测、物理隔离不再是保护信息安全的法宝。

（7）无线上网、移动通信、活动硬盘在给人们带来方便和高效的同时，随时有可能被截取、仿冒、侦听。

（8）笔记本式计算机使用便捷，但人们也开始意识到由于遗失、被盗带来的泄密现象的严重性。

因此，我们需要对信息内容本身进行安全防范，做到防止复制，防止二次传播，这样的信息安全技术才是真正可靠的技术。对企业机密信息管理来说，

需要考虑信息内容本身的安全。

一般说来，计算机网络存在着如表 9-2 所示的安全风险及需要采取的安全对策。

表 9-2　安全风险及对策

项目	风　　险	安 全 对 策
用户风险	身份假冒	身份认证
	身份窃取	身份认证
	非授权访问	访问授权管理
	重放攻击	鉴别、记录、预警
	否认	审计、记录
	深度入侵	预警、阻断
	端点安全	端点准入防御（EAD）
数据风险	窃取	实体安全、加密
	篡改	完整性检验
	毁坏	灾难恢复
	有害数据侵入（包括病毒等）所造成的破坏	检测、过滤、分析、捕获
用户和服务风险	非授权访问	访问授权
	身份假冒	身份认证
	密钥管理漏洞	CA、KDC、PKI
	数据库自身的漏洞	检测、打补丁、升级
	操作系统自身的漏洞	漏洞检测、打补丁、升级
	服务的脆弱性及漏洞	检测、打补丁、更新
	应用系统自身的缺陷	更新完善
服务器风险	入侵探测	实时监测、预警、回火
	非授权访问	访问控制
	策略漏洞	策略管理、检查
	系统配置缺陷	升级、自检报告
	系统版本	检测、更新
	系统平台	评测、选择
	实体安全缺陷	防辐射、防橇、防雷击
	服务器所存在的陷门和隐通道	尚无相应的解决技术及产品
网络风险	入侵探测	检测、预警、回火
	设备攻击	实时监测、管理、维护
	通道保密强度	采用高强度加密产品
	网络设备配置缺陷	定期检测、加强配置管理、日志、审计
	网络设备物理安全缺陷	更新
	网络设备存在的陷门和隐通道	尚无相应的解决技术及产品
	网络设备实体的安全	防盗、防辐射、防雷击

表 9-2 具体描述了数据安全的问题，基本上可以通过加强网络安全、操作系统安全等实现，然而其中超过 85%的安全威胁来自企业内部。作为企业机密

管理者肯定知道，真正核心数据防扩散技术，需要对信息内容本身先进行加密，然后在此基础上再进行安全防范，做到防止复制，防止二次传播，这样的信息安全技术才是真正可靠的技术。所以，针对企业机密信息管理来说，我们重点需要考虑信息内容本身的安全。

9.6.2 数据备份安全

当我们拥有一个贵重的物品时，需要对其进行保存，在这个过程中需要考虑这些问题：首先这个物品不能损坏，否则其价值就损坏了，这样就需要将其存放在特别牢固的地方，避免发生意外；其次还要防止这个物品被盗窃，否则其价值就被转移了，这样就需要对其存放地点进行防盗处理。当然以上这些存放和防盗的花费肯定要低于物品本身的价值才有意义，而破解防盗技术所需的花费要大于物品价值才能有效。

如今信息大量以电子文档形式进行处理、存放和传输，其中大量的数据也具有非常重要的价值，有些数据的价值可能占据公司价值的一个很大比例。为此，我们同样需要考虑这些数据的处理、存放和传输过程中需要防止损坏和被盗等事件发生，这就要求我们针对数据损坏（价值损坏或消失）和被盗（价值转移）具有不同的处理方式。

9.6.3 防止数据的损坏

如今，企业机密信息大量以电子文档方式存在，而电子文档主要存放在磁盘上。目前虽然磁盘相对比较稳定，但是大量的信息都存放在磁盘上，一旦发生损坏，如果数据只有这个损坏磁盘上的一个拷贝，那么将会完全丢失，在这些信息已经成为极其重要资产的现代社会，对一个企业来说，严重情况下将是致命的。9•11 事件发生之后，世贸大厦中那些没有数据灾难备份的公司纷纷倒闭，而那些考虑到数据容灾的公司，在灾难发生几天到个把月的时间就恢复业务运行了，可见数据可靠是多么的重要。

1. 数据可靠需要考虑的问题

（1）主要先考虑数据磁盘发生故障时数据的可靠，这里主要可以应用 RAID 系统来解决。RAID 的初衷主要是为大型服务器提供高端的存储功能和冗余的数据安全。在系统中，RAID 被看作是一个逻辑分区，但是它是由多个（最少两块）硬盘组成的。它通过在多个硬盘上同时存储和读取数据来大幅提高存储系统的数据吞吐量（Throughput），而且在很多 RAID 模式中都有较为完备的相互校验/恢复措施，甚至是直接相互的镜像备份，从而大大提高了 RAID 系统的容错度，提高了系统的稳定冗余性，这也是 Redundant 一词的由来。

在这些数据价值远远大于用于存放数据的磁盘价值的今天，通过增加磁盘

数量（降低硬盘的利用率）来保障数据安全是非常值得的。

一般可以考虑使用 RAID 1、RAID 3、RAID 5 和 RAID 6 等技术。详述如下：

① RAID 1：Mirroring and Duplexing（相互镜像）。将数据同时存放在两个硬盘上，这样虽然硬盘的利用率降低了 50%，但是数据的可靠性增加了一倍。

② RAID 3：Parallel transfer with parity（并行传输及校验）。就是在多个硬盘构成的系统中，使用一个独立的硬盘作为系统校验盘，将其他硬盘上的数据进行异或（XOR）运算后存放在此校验盘上，当整个系统只有一个硬盘发生故障时，故障盘上的数据可以通过其他数据硬盘和校验硬盘上的数据进行异或（XOR）运算重新算出来，保障了数据的可靠使用。这个过程需要一个独立的硬盘存放，虽然浪费了一个硬盘的容量，但可以保障只损坏一个硬盘的时候数据的安全。

③ RAID 5：RAID 5 和 RAID 3 相似（所以硬盘利用率和数据可靠性相同）但避免了 RAID 3 的瓶颈，方法是不用独立的校验磁盘而将校验数据以循环的方式放在每一个磁盘中。RAID 5 的控制比较复杂，尤其是利用硬件对磁盘阵列的控制，因为这种方式的应用比其他的 RAID 级别要掌握更多的事情，有更多的输出/输入需求，既要速度快，又要处理数据、计算校验值、做错误校正等，所以价格较高，其应用最好是 OLTP，至于用于大型文件，则不见得有最佳的性能。

RAID 5 在不停机及容错方面的表现都很好，但如有磁盘故障，对性能的影响较大，大容量的快取内存有助于维持性能，但在 OLTP 的应用上，因为每一笔数据或记录（record）都很小，对磁盘的存取频繁，故有一定程度的影响。RAID 5 要做的事情太多，所以价格较贵，不适于小系统，但如果是大系统使用大的磁盘阵列的话，RAID 5 却是最便宜的方案。

RAID 6：RAID 6 是 RAID 家族中的新技术，是在 RAID 5 基础上扩展而来的，因为在上面的 RAID 技术中，出现损坏两块硬盘的情况下，数据安全还是不能得到保障了，所以出现了 RAID 6 技术。同 RAID 5 一样，数据和校验码都是被分成数据块，然后分别存储到磁盘阵列的各个硬盘上。RAID 6 加入了一个独立的校验磁盘，它把分布在各个磁盘上的校验码都备份在一起，这样 RAID 6 磁盘阵列就允许两个磁盘同时出现故障了，这对于数据安全要求很高的应用场合是非常必要的。这样搭建一个 RAID 6 磁盘阵列最少需要四块硬盘。但是 RAID 6 并没有改善 RAID 5 写入性能不佳的情况，写入缓存的应用仅仅能对这个缺点进行一定程度的弥补，并不能从根本上解决问题。因为 RAID 5 和 RAID 6 都可以根据应用程序来更改数据块的大小，所以 RAID 6 的实际性能还会受到这个因素的影响。

在实际应用中 RAID 6 的应用范围并没有其他的 RAID 模式那么广泛。如果实现这个功能一般需要设计更加复杂、造价更昂贵的 RAID 控制器，所以它一般也不会集成在主板上。总的来说，RAID 6 是可以容忍两块硬盘同时出现故障而仍然可以恢复出数据的，另外它的实际容量是总容量减两块硬盘容量，如五块 80GB 的硬盘来做 RAID 6，那么它的实际可用容量就是 80GB×5–80GB×2

了，为 240GB。

既然 RAID 6 是最新的 RAID 冗余技术，那么它的性能应该是非常不错的。RAID6 的性能：

a. RAID 6 的随机读取性能：很好（当使用大数据块时）。

b. RAID 6 的随机写入性能：差，因为不但要在每块硬盘上写入校验数据而且要在专门的校验硬盘上写入数据。

c. RAID 6 的持续读取性能：好（当使用小数据块时）。

d. RAID 6 的持续写入性能：一般。

e. RAID 6 的优点：快速的读取性能，更高的容错能力。

f. RAID 6 的缺点：很慢的写入速度，RAID 控制器在设计上更加复杂，成本更高。

（2）存储系统完成之后，我们需要考虑整个网络系统数据的可靠。RAID 技术保障了存储系统中硬盘出现故障时数据的可靠，但是当今数据往往在网络上使用，仅仅存储系统数据可靠，但网络出现故障引起数据不能使用也是不能允许的，这就需要考虑整个网络系统的问题。

随着计算机的激增，大量的不兼容性导致数据的获取日趋复杂。因此采用广泛使用的局域网加工作站簇的方法就对文件共享、互操作性和节约成本有很大的意义。NAS 包括一个特殊的文件服务器和存储。

NAS 服务器上采用优化的文件系统，并且安装有预配置的存储设备。由于 NAS 是连接在局域网上的，所以客户端可以通过 NAS 系统与存储设备交互数据。

一个存储网络是一个用在服务器和存储资源之间的、专用的、高性能的网络体系，它为了实现大量原始数据的传输而进行了专门的优化。因此，可以把 SAN 看成是对 SCSI 协议在长距离应用上的扩展。

SAN 的市场主要集中在高端的、企业级的存储应用上，这些应用对于性能、冗余度和可获得性都有很高的要求。

当对 SAN 和 NAS 进行比较时，这两种相互竞争的技术实际上是互补的。SAN 和 NAS 是在不同用户需求的驱动下的独立事件。SAN 是以数据为中心的，而 NAS 是以网络为中心的。概括来说，SAN 具有高带宽块状数据传输的优势，而 NAS 则更加适合文件系统级别上的数据访问。

目前 DAS、SAS（Server Attached Storage）、SAN 和 NAS 之间的区别正在变得模糊，所有的技术都需在用户的存储需求下接受挑战。传统的客户端服务器的计算模式将会演化成具有任意连接性的全球存储网络。在这种情况下，数据的利用率会得到提高，分布式数据也会得到更加优化的存储。

只有采用了存储虚拟化的技术，才能真正屏蔽具体存储设备的物理细节，为用户提供统一集中的存储管理。采用存储虚拟化技术，用户可以实现存储网络的共用设施目标如下：

① 存储管理的自动化与智能化：在虚拟存储环境下，所有的存储资源在逻辑上被映射为一个整体，对用户来说是单一视图的透明存储，而单个存储设备

的容量、速度等物理特性却被屏蔽掉了。

② 提高存储效率：主要表现在消除被束缚的容量，整体使用率达到更高的水平。

③ 减少总体拥有成本（TCO），增加投资回报（ROI）：采用存储虚拟化技术，可以支持物理磁盘空间动态扩展，这样用户现有的设备不必抛弃，可以融入到系统中来，保障了用户的已有投资，从而降低了用户 TCO，实现了存储容量的动态扩展，增加了用户的 ROI。

9.6.4 防止数据被盗

谈到对信息内容进行加密，我们一般首先想到的是运用一些常见的加密软件对敏感的文件或数据设置密码，这样在访问这些文件的时候就需要知道这些文件的访问密码，通过输入正确的密码，才能访问这些文件或数据。每次保密前要设置密码，查看时也要输入解密码，费时费力不说，较大的弊病是这一切都要靠我们人为主动地、有意识地去保密。但试想一下，当一个本企业的内部人员（他本身平时就能经常接触这些资料）想带出该企业的一些核心资料的话，他完全可以不主动去加密这些文件（就算加密了，因为他需要处理这些数据，当然也知道密码，加密了对于这样的人也是没有用的），从而将这些重要的资料一次性大批量的复制走了。这样的加密技术，对于预防企业内部人员的泄密，又有多大的作用呢？

所以，对于企业核心数据防扩散加密软件，它必须具备以下几个基本条件：

1. 加密的强制性

不管你愿意还是不愿意，企业内部产生的一些核心数据都要被强制性的加密，而且在生成文件时就对产生的文件进行强制性保护控制。

2. 加密解密的方便性（无密钥加密）

时间是宝贵的，我们不希望每次加密文件时输入密码，查看文件时也要输入密码。我们希望核心数据防扩散加密软件能够自动辨识出哪些是本单位并经过授权的计算机，记住这些计算机的硬件环境。在这些计算机上，我们无需输入密码就可以轻松打开文件（这样“内贼”也就不知道如何解密了），因为我们文件的解密码就是这些经过授权的计算机的硬件环境，而且只有在企业内部网络环境中才能自动解密，出了这个环境就无法解密了。

3. 加密解密的自动性和快捷性

我们的要求是，在这些重要数据产生的时候，我们的加密软件必须要能实时自动跟踪并对这些文件进行自动加密，打开文件的瞬间，对这些文件进行自动解密，整个加密过程无需人工干预。就是打开一个未加密文件时，不管有没

有对该文件进行编辑，都能够自动对该文件进行加密，并且不影响应用程序的正常运行及文件的正常使用。加密状态的文件在计算机上可以双击直接打开，并可以对它们进行正常的编辑和修改，使用上和没加密的普通文件没有任何区别。系统在后台自动运行，对使用人员是透明的，不需任何操作动作。不改变已有的使用习惯，生成的加密文件对设计系统不产生任何影响。在同一公司内部只要都安装了同一系统的计算机上，文件可以正常流通，不受到限制。

4. 加密资料的安全性和唯一性

企业的一些核心数据是企业的无形财富。为了更安全地保护这些资料，必须要求加密技术的高强度性，加密了的文件无法被破解（破解所需的花费要远远大于数据价值）。同时，还要确保同样用这种核心数据防扩散加密软件，企业的资料不能互相打开，这就是每个单位资料解密密钥的唯一性。

5. 方便对外交流

当企业需要对外交流时，某些密级不高的文件需要解密（但是需要高层领导审核，普通员工不能对任何文件进行解密操作），这就需要方便高层领导对部分需要解密的文件进行解密操作。

9.7 灾难备份与恢复

当应用系统的一个完整环境因灾难性事件（如火灾、地震等）遭到破坏时，为了迅速恢复应用系统的数据、环境，使应用系统恢复运行，需要异地灾难备份系统（也称容灾系统）。可以说，对于关键事物的处理系统，如企业的各项业务系统（客户服务、计费、ERP、BI、CRM、IDC 等），建立最高级别的安全体系，也是提高服务质量、在竞争中立于不败之地的重要举措。

9.7.1 容灾技术的意义

长期以来，对企业而言，建立一套可行的容灾系统相当困难，主要是高昂的成本和技术实现的复杂度。鉴于此，从可行性而言，容灾系统必须具有良好的性能价格比。

建立异地容灾系统，即指建立远程的数据中心，通过配置远程容灾系统将本地数据实时进行远程复制，同时实现本地系统故障时应用系统的远程启动，确保系统的不中断运行。

建立异地容灾中心的优势在于：

（1）强大的一级灾难抗御能力；

（2）有效防止物理设备损伤产生的灾难后果；

（3）提供 99.9999%的安全机制；

（4）实时数据复制提供强大的数据交换能力。

集群（cluster）是两台或更多台计算机（结点）在一个群组内共同工作。与单独工作的计算机相比，集群能够提供更高的可用性和可扩充性。随着数据安全技术的发展，具有高可用的集群技术越来越成熟，部署得越来越普及，它确实解决了用户系统的高可用性问题，为业务的良性发展提供了稳定的基石。随着业务的发展，商业环境对服务供应商提出的要求也越来越苛刻，这必将使应用系统及其数据对高可用性的要求走上一个新的台阶。

一个本地集群系统理论上可以提供 99.99%以上的系统高可用性，但一旦发生火灾、自然灾害、人为破坏等意外事件，企业将如何应对呢？如果没有必要的准备和应对手段，这样的一次意外对企业来说将是灾难性的。要提高自己的抗灾能力，企业必须建立起一个容灾系统。

9.7.2 容灾技术的分类

一个容灾系统的实现可以采用不同的技术。一种技术是采用硬件进行远程数据复制，称为硬件复制技术。这种技术的提供者是一些存储设备厂商。数据的复制完全通过专用线路实现物理存储设备之间的数据交换。另一种技术是采用软件系统实现远程的实时数据复制，并且实现远程的全程高可用体系（远程监控和切换）。这种技术的代表是 VERITAS 等一些著名存储软件厂商。下面的章节会对以上两种技术进行详细的论述。

从另一个方面来说，容灾系统的归类要由其最终达到的效果来决定。从其对系统的保护程度来分，可以将容灾系统分为数据容灾和应用容灾。

所谓数据容灾，就是指建立一个异地的数据系统，该系统是本地关键应用数据的一个实时复制。在本地数据及整个应用系统出现灾难时，系统至少在异地保存有一份可用的关键业务的数据。该数据可以是本地生产数据的完全实时复制，也可以比本地数据略微落后，但一定是可用的。

所谓应用容灾，是指在数据容灾的基础上，在异地建立一套完整的与本地生产系统相当的备份应用系统（可以是互为备份）。建立这样一个系统相对比较复杂，不仅需要一份可用的数据复制，还要有网络、主机、应用、甚至 IP 等资源，以及各资源之间的良好协调。应用容灾应该说是真正意义上的容灾系统。

数据容灾（包括硬件容灾方案和软件容灾方案）又称为异地数据复制技术，按照其实现的技术方式来说，主要可以分为同步传输方式和异步传输方式（各厂商在技术用语上可能有所不同）。而根据容灾的距离，数据容灾又可以分成远程数据容灾和近程数据容灾方式。下面，我们主要按同步传输方式和异步传输方式对数据容灾展开讨论，其中也会涉及远程容灾和近程容灾的概念，并做相应的分析。

1．同步传输的数据复制

有关同步数据容灾，从传统意义上讲，就是通过容灾软件（可以含在硬件系统内）将本地生产数据通过某种机制复制到异地。从广义上讲，同步数据容灾是指在异地建立起一套与本地数据实时同步的异地数据。

采用同步传输方式进行异地数据容灾的过程如下：

（1）本地主机系统发出第一个 I/O 请求 A；

（2）主机会对本地磁盘系统发出 I/O 请求；

（3）本地磁盘系统完成 I/O 操作，并通知本地主机“I/O 完成”。

（4）在往本地 I/O 的同时，本地系统（主机或磁盘系统）会向异地系统发出 I/O 请求 A；

（5）异地系统完成 I/O 操作，并通知本地系统“I/O 完成”；

（6）本地主机系统得到“I/O 完成”的确认，然后发出第二个 I/O 请求 B。

不同的异地数据复制技术的实现方式是不同的，其包括：

（1）基于主机逻辑卷层的同步数据复制方式（软件复制方式）；

（2）基于磁盘系统 I/O 控制器的同步数据复制方式（硬件复制方式）。

首先，描述基于主机逻辑卷层的同步数据复制方式。

基于主机逻辑卷层的同步数据复制方式以 VERITAS Volume Replicator（VVR）为代表，VVR 是集成于 VERITAS Volume Manager（逻辑卷管理）的远程数据复制软件，它可以运行于同步模式和异步模式。在同步模式下，当主机发起一个 I/O 请求 A 之后，必然通过逻辑卷层，逻辑卷管理层在向本地硬盘发出 I/O 请求的同时，将通过 TCP/IP 网络向异地系统发出 I/O 请求。其实现过程如下：

（1）本地主机系统发出第一个 I/O 请求 A；

（2）主机逻辑卷层会对本地磁盘系统发出 I/O 请求；

（3）本地磁盘系统完成 I/O 操作，并通知本地逻辑卷层“I/O 完成”；

（4）在往本地磁盘系统 I/O 的同时，本地主机系统逻辑卷层会向异地系统发出 I/O 请求 A；

（5）异地系统完成 I/O 操作，并通知本地主机系统“I/O 完成”；

（6）本地主机系统得到“I/O 完成”的确认，然后发出第二个 I/O 请求 B。

其次，考察基于磁盘系统 I/O 控制器的同步数据复制功能。

基于磁盘系统的同步数据复制功能实现异地数据容灾，如 SRDF 和 PPRC。这两个软件运行的平台是磁盘系统，部署这样的系统必须要求在两端采用相同种类的磁盘系统。

基于磁盘系统的同步数据复制是：当主机发出一个 I/O 请求 A 之后，I/O 进入磁盘控制器，该控制器在接到 I/O 请求后，一方面会写入本地磁盘，同时利用另一个控制器（或称通道），通过专用通道（如 ESCON）、FC 光纤通道（IP over FC）或者租用线路，将数据从本地磁盘系统同步地复制到异地磁盘系统。

其实现过程如下：

（1）本地主机系统发出第一个 I/O 请求 A；

（2）主机对本地磁盘系统发出 I/O 请求；

（3）在往本地磁盘系统 I/O 的同时，本地磁盘系统会向异地磁盘系统发出 I/O 请求 A；

（4）本地磁盘系统完成 I/O 操作；

（5）异地系统完成 I/O 操作，并通知本地磁盘系统“I/O 完成”；

（6）本地磁盘系统向主机确认“I/O 完成”，然后主机系统发出第二个 I/O 请求 B。

2. 同步数据容灾的性能分析

利用同步传输方式建立异地数据容灾，可以保证在本地系统出现灾难时，异地存在一份与本地数据完全一致的数据备份（具有完整的一致性）。但利用同步传输方式建立这样一个系统，必须考虑“性能”这个因素。

采用同步数据传输方式时，从前面的描述来看，本地系统必须等到数据成功地写到异地系统，才能进行下一个 I/O 操作。一个 I/O 通过远程链路写到异地系统，涉及三个技术参数：带宽、距离和中间设备及协议转换的时延。

在 1000km 距离上，允许的最大 I/O 量在不存在带宽限制时，已经远远低于本地 I/O 的能力。（注：上面分析还未考虑中间设备及协议转换的延时）

中间链路设备和协议转换的方式不同，时延不同，对性能的影响也不同。在对性能影响的分析中，这个因素也应计算在内。表 9-3、表 9-4、表 9-5、表 9-6 显示了介质、协议和大概时延的比较，这里提供的数据只精确到微秒级，仅供参考，实际数据应该向设备供应商索取。

表 9-3 数据线路处理时延估计

链路设备和协议	带　　宽	支持的距离	设备和协议转换时延
租用线路	任意	不受限制	≈1ms
ESCON	136Mbit	66km	$<100\mu s$
LAN	1000Mbit	10km	$<100\mu s$
ATM	655Mbit	不受限制	$<100\mu s$
IP over FC	800Mbit	60km	$<100\mu s$
FC	800Mbit	60km	$<10\mu s$

表 9-4 数据传输距离时延

	距离		
	1000KM	**100KM**	**10KM**
线路时延/次 I/O	6ms	$600\mu s$	$60\mu s$
支持的链路和协议	租用线路 ATM	租用线路 ATM	租用线路 ATM ESCON LAN IP over FC FC
本地磁盘 I/O 能力	10KB/ms		

表 9-5　线路系统考察

	1000km		100km	
	租用线路	ATM	租用线路	ATM
线路时延/次 I/O	6ms	6ms	600μs	600μs
设备和协议时延	> 1ms	< 100μs	> 1ms	< 100μs
每个 I/O 响应时间	> 8ms	> 7ms	> 2.6ms	1.7ms
	不适合用同步传输方式			
备注	不适合用同步传输			

注：在 1000km 和 100km 距离上，采用租用线路和 ATM 允许的最大 I/O 能力（假定带宽足够，数据块大小以 10KB 为例）。

表 9-6　等距离条件下的时间延时

	10km			
	租用线路	ATM/LAN	ESCON，IP over FC	FC
线路时延/次	60μs	60μs	60μs	60μs
设备协议时延	> 1ms	< 100μs	< 100μs	< 10μs
I/O/（次数/s）	485～930	900～5800	900～5800	900～12500
I/O/（MB/s）	4.8～9.3	9～58	9～58	9～125
备注		适合用同步传输		

注：在 10km 距离上，采用各种传输协议允许的最大 I/O 能力，数据块大小以 10KB 为例（假定带宽足够）。

3．异步数据复制

从前面的分析来看，同步数据容灾一般只能在较短距离（10～100km）内部署，大于这个距离，就没有实际应用价值了。因为在 1000km 距离上，4.5MB/s 的速率即使将数据复制到异地，每个 I/O 的响应时间也会超过 10ms，这种响应速度太慢了。

异步数据容灾是在“线路带宽和距离能保证完成数据复制过程，同时，异地数据复制不影响生产系统的性能”这样的要求下提出来的。考虑异步数据容灾，应该注意以下几个技术条件和事实：

（1）带宽必须能保证将本地生产数据基本上完全复制到异地容灾端，还要考虑距离对传输能力的影响。

（2）按照前面的估算，在 1000km 范围内，一条带宽足够的线路能支持的 I/O 流量最大为（数据块大小为 10KB）：1.4MB×3600s×24h=120GB/d。

（3）异地容灾远端数据会比本地生产端数据落后一定时间，这个时间随采用的技术，带宽、距离、数据流特点的不同而不同。一般而言，软件方式的数据复制技术具有完整的数据包的排队和断点重发机制，在灾难情况下可以保证灾难时间点的数据一致性。

（4）异步容灾基本不影响本地系统性能。

与同步传输方式相比，异步传输方式对带宽和距离的要求低很多，它只要求在某个时间段内能将数据全部复制到异地即可，同时异步传输方式也不会明

显影响应用系统的性能。其缺点是在本地生产数据发生灾难时，异地系统上的数据可能会短暂损失（如果广域网速率较低，交易未完整发送的话），但不影响一致性（类似本地数据库主机的异常关机）。

通过异步传输模式进行异地数据复制的技术包括以下方式：

（1）基于主机逻辑卷层的数据复制方式；

（2）基于磁盘系统 I/O 控制器的数据复制方式。

首先申明：针对异步传输模式，这里以 VERITAS VVR 为例说明，但并不表示所有基于主机进行复制的其他软件采用同样方式，也不保证其他软件是有应用价值的。

VERITAS VVR（Volume Replicator）通过基于 Volume 和 Log 的复制技术，保证在任何时刻本地系统发生自然灾难时，在异地的数据仍是可用的。

VERITAS VVR 在异步模式下采用了 Log 技术来跟踪未及时复制的数据块，这个 Log 是一个先到先服务的堆栈，每一笔 I/O 处理都会首先放进这个 Log，并按到达先后顺序复制到异地服务器系统，

VERITAS VVR 采用的 I/O 控制机制是支持先到先服务的 Log 技术，因此，不管异地数据比本地数据落后多少时间，都能保证异地数据库数据的一致性。比如，本地系统在 12：00 时发生自然灾难，由于部分数据未被及时复制到异地，如有 10min 的数据未完成复制，那么在异地系统上存在 11：50 以前的所有数据，且这个数据库是可用的。

目前的基于磁盘系统的异地数据复制技术采用 Bitmap 技术和 Timestamp 技术，这两种技术都不能保证本地向异地复制数据的顺序严格和本地 I/O 的顺序相同，所以，这两种方式都不能保证异地数据库的完整性。

Bitmap（位图）技术记录未被及时复制的数据块的方法是：对于每个数据块（如 32KB）用一个 bit 来对应，某一个 bit 被置为“1”时，表示其对应的数据块已被修改过，正在等待处理（这里是等待被复制）。由此可以看出，当有一块以上的数据块未被及时复制时，系统并无法确认哪一块数据块应该先复制到异地，所以，系统将任选一块，即不按到达的时间先后进行复制。可以看出，这种方式不能根本保证异地数据库数据的完整性、一致性。

Timestamp 方式是对每个未及时传送的数据块盖上一个时间戳。从表面上看，由于时间戳的关系，好像能确定一个数据块被修改的时间顺序了。其实不然，当一个未被及时复制的数据块被第 2 次修改并盖上新的时间戳时，数据复制的顺序就被破坏了。例如：

现在有 10 块数据块未被复制，编号“1、2、3、4、5、6、7、8、9、10”，若第 3 块数据被再次修改，并被盖上一个新的时间戳“11”，那么系统会按“1、2、（没有 3）、4、5、6、7、8、9、10、11”的次序进行复制。存储工程师可以看到，在复制进行到“4～10”之间时，异地数据的完整性被破坏了。

事实上，在一个运行繁忙的系统中，出现这种情况的机率极高，甚至每时每刻都处在这种状态之下。所以，本着严格的、对系统可用性负责任的态度，

可以认为 Timestamp 技术虽然比 Bitmap 技术有一定优势，但实际上也无法保证异地数据的完整性和可用性。

Bitmap 和 Timestamp 方式的技术弱点是没有 Log。

作为磁盘系统内置的数据复制功能，传统的磁盘管理模式没有考虑在磁盘系统内部开辟出一个磁盘块给磁盘系统控制器本身使用，所以，磁盘系统无法采用 Log 模式进行异步数据复制。

磁盘系统保留异步传输模式的目的是复制，但不是容灾复制。

数据复制的目的不仅仅是容灾。数据容灾要求两地时时保持连接，数据复制过程在任一时间都在进行（除非有线路或设备故障）。而非容灾性复制只要求在某一个时间段里将数据复制到异地，复制告一段落后（在某一时刻完全同步），复制工作会暂停。这种复制可能是为一个特殊目的只做一次，如在线业务迁移；也可能每天或每月追加一次。这样，在异地就会存在一份最大损失数据量为一天或一个月的生产数据复制品，其对数据的保障能力，如同磁盘备份。这种方式复制数据的目的包括：① 在异地保存一份备份数据（如同磁盘备份异地保存）；② 在线业务迁移，当信息中心或其中的一个服务要迁移到另一个地方，又希望少停机时（实际上也可用磁盘备份和恢复来实现）；③ 利用与磁盘快照技术结合，为异地开发中心提供一个与生产数据尽量相同的测试数据源。当然，也可用于其他可能的目的。

综上所述，可以看出，虽然基于磁盘系统的异地数据复制功能有异步传输模式，但实际上并不支持异步数据容灾，只有像 VERITAS Volume Replicator 这样基于先进先出的 Log 技术的解决方案才真正支持异步数据容灾。

4. 软件容灾方式

广域网络的高可用技术，一般是软件容灾方式。它支持应用容灾，即应用系统的完全高可用和远程切换系统，这里指一整套完整的本地高可用系统和异地高可用系统的完整结合体系。本地的高可用系统指在多个服务器运行一个或多个应用的情况下，应确保任何服务器出现任何故障时，其运行的应用不能中断，应用程序和系统应能迅速切换到其他服务器上运行，即本地系统集群和热备份。

而远程的容灾系统中，除了本地系统的安全机制外，还应具有广域网范围的远程故障切换能力和故障诊断能力。实际上，广域网范围的高可用能力与本地系统的高可用能力应形成一个整体，实现多级的故障切换和恢复机制，确保系统在各个范围的可靠和安全。

广域网体系的远程故障切换机制的流程（软件方式）如下：

（1）本地系统的故障分级、常规级别在本地系统进行高可用切换，如网卡故障、应用系统故障、文件系统故障（本地 cluster）。

（2）高级别故障（如火灾、地震）通过远程监控体系和报警体系实现远程切换（异地 cluster）。切换包括 IP、域名、应用等。

一旦故障解除，恢复体系如下：

（1）应用系统实现主备站点的恢复传输。

（2）异地复制中断传输的恢复流程（软件方式复制）。

（3）断点序号重传或增量异地同步实现增量块复制。

9.7.3 小结

表 9-7 对于各种容灾技术的工作方式进行了总结。

表 9-7 容灾比较列表

项　　目	Software（同步）	Software（异步）	基于阵列的同步数据容灾
理想距离	< 100km	< 1000km	60km (光纤)
链路要求	任何支持 TCP/IP 的设备	任何支持 TCP/IP 的设备	ESCON、ATM IP over FC
理想链路带宽	> 40Mbit	相对较小	> 40Mbit
对应用系统性能的影响	很大	很小	很大
是否需要专用磁盘系统	不需要	不需要	必须
部署的简单性	长距：复杂 短距：一般	一般	硬件：复杂 软件：一般
维护的简单性	一般	简单	一般
造价	中等	中等	很高
涉及软件	VVR	VVR	阵列内置

根据以上的分析可以看出，硬件系统的容灾技术（指磁盘阵列）在对主机系统的内部开销上较小，但是十分影响本地 I/O 的性能，同时要求本地和异地均采用专用的磁盘阵列，成本和造价极高。比较重要的是，这种方式的传输距离有限，仅限于同城传输。

采用软件的数据复制方式（如 VVR），一般为异步方式。这种方式具有对本地系统 I/O 影响很小、传输距离长的优势，并且可以支持任意磁盘阵列，使得造价相对较小。其不足是如果线路速率较慢，会造成故障时轻微数据受损。

9.8 内容安全

内容安全是网络信息安全的最终目标，是企业信息系统安全体系建设的关键指标之一。“信息内容”涉及动画、游戏、影视、数字出版、数字创作、数字馆藏、数字广告、互联网、信息服务、咨询、移动内容、数字化教育、内容软件等，主要可分为政务型、公益型、商业型三种类型。

信息内容的定义来源于数字内容产业。一般来说，“信息内容产业”指的是基于数字化、网络化，利用信息资源创意、制作、开发、分销、交易的产品和

服务的产业。

随着互联网的普及，信息内容的种类与数量急剧膨胀，其中鱼目混杂，反动言论、盗版、淫秽与暴力等不良内容充斥其间。由于信息内容安全涉及国家利益、社会稳定和民心导向，因此，受到各方的普遍关注。

信息内容安全包括以下两个方面：

（1）数字信息资源内容的安全性；

（2）对有害信息资源内容的可控性。

以下就企业内容安全的必要性，内容安全的分类和解决方案逐一阐述。

9.8.1　保障内容安全的必要性

随着数字信息的膨胀性发展，在信息资源的开发利用中催生了新的产业——数字内容产业。数字内容产业定义为基于数字化、网络化，利用信息资源创意、制作、开发、分销、交易的产品和服务的产业，它涉及动画、游戏、影视、数字出版、数字创作、数字馆藏、数字广告、互联网、信息服务、咨询、移动内容、数字化教育、内容软件等等。

这要求保护合法信息资源的版权和应得的利益，以及实现对有害信息资源内容的可控性；针对网络上充斥着宣扬反动、色情、暴力、犯罪的内容进行有效监管，并且对社会危害信息进行合法管制。

内容安全主要面临的威胁有以下几个方面：

（1）政治性：来自国内外反动势力的攻击、诬陷和西方的和平演变图谋；

（2）健康性：色情、淫秽内容和暴力等；

（3）保密性：国家和企业机密被窃取、泄露和流失；

（4）隐私性：个人隐私被盗取、倒卖、滥用和扩散；

（5）产权性：知识产权被剽窃、盗用等；

（6）防护性：病毒、垃圾邮件、网络蠕虫等恶意信息耗费网络资源。

在具备大量人群集聚的互联网或企业内部网络上，有产生信息和消费信息的十分活跃的人群。因此，我国大中型企业的企业信息系统在内容安全方面，随着时代和技术的进步、发展，还会呈现更多不确定的挑战。为此，保护内容安全，是企业信息系统安全架构的难点和重点。

9.8.2　内容安全的分类

1．违禁内容的传播

违禁内容是指内容本身要表达的意思违反了某种规则或安全策略，尤其是政策法规的范畴。

在很多情况下，违禁内容的表达方式和格式并没有什么问题，无法从表达

方式或格式来加以禁止，必须从语意和关键词上理解该内容是违禁的。

违禁内容的传播属于内容安全的范畴，而不是网络安全的范畴。违禁内容的危害是对思想造成破坏。

该方面的特点包括以下内容：

（1）网络的匿名性；

（2）网络的可复制性；

（3）检验网络真实的间接和滞后性；

（4）传播速度快捷，具有全球化、超地域的社会覆盖面；

（5）网络竞争压力。

2．基于内容的破坏

基于内容的破坏，大家比较容易理解，如病毒。一个文件感染了病毒，对用户的计算机和网络会造成破坏。影响力比较大的病毒案例如下：

（1）“耶路撒冷”病毒；

（2）Nyxem 病毒；

（3）CIH 病毒；

（4）熊猫烧香病毒。

对于网络而言，感染了病毒的文件与正常的文件在差异性方面可以通过技术手段借助专业特征库来实时识别和跟踪，在符合一定约束条件后，采取技术处理措施。

3．基于内容的攻击

基于内容的攻击是一种攻击行为，载体是内容，攻击的对象是应用程序，目标是取得对应用主机的控制权，攻击主机。

4．针对操作系统和应用软件漏洞的攻击

操作系统和应用软件漏洞的发作方式可以体现为：在 Web 上的表格填写数据时，填写恶意格式，导致 CGI 程序执行错误，引发应用程序出错。例如：

（1）SQL Slammer 病毒；

（2）MSBlaster 病毒；

（3）钓鱼软件。

9.8.3 内容安全解决方案

内容安全解决方案分为以下几个部分描述：

1．禁止违禁内容传播的解决方案

针对禁止违禁内容传播的解决方案，主要技术路线是对违禁内容进行内容

过滤。例如，基于关键词的内容过滤和基于语意的内容过滤。前者在技术上很成熟，准确度很高，漏报率低，但误报率高；后者在技术上还不成熟，存在很多困难，效率低下，实现目标困难。

对违禁内容的来源进行访问控制，这种方式对已经知道恶意传播的对象非常有效。到目前为止，还没有禁止违禁内容传播的理想的理论方法，就像天气或地震预报一样，总是尽可能的准确，但无法绝对准确。在必须执行违禁内容控制的情况下，多采用人工和技术相结合的策略。

对违禁内容传播的预警，包括内容监管、信息公开、对数字信息的版权保护。

2. 防止基于内容破坏的解决方案

防病毒是目前采用最多的防止基于内容破坏的解决方案，通过查找内容中的恶意病毒代码来消除基于内容的破坏。防病毒软件同样存在漏报和误报的问题。

最关键的问题是，每次总是病毒爆发在前，才能取得病毒特征代码，然后才能防止该病毒。预防已知病毒的实现较为成功，但预防未知病毒的能力较弱。

为了解决防病毒软件这方面的不足，出现了很多的相关技术如专家会诊、引发病毒隔离区等，来补充和弥补病毒软件的不足。

3. 防止基于内容攻击的解决方案

基于内容的攻击的危害已经超过违禁内容传播和病毒的危害，成为目前最热门的威胁之一。

目前存在的十大漏洞和风险包括：① 参数无效；② 访问控制失效；③ 账户和会话管理失效；④ 跨站点脚本；⑤ 缓冲溢出；⑥ 恶意命令；⑦ 错误处理问题；⑧ 不安全加密；⑨ 远程管理缺陷；⑩ 配置错误。

针对应用安全代理产品解决部分基于内容攻击的问题，应用安全代理将应用与安全进行适当的分工，应用专注功能的问题，将安全问题交给专业厂商来完成。

9.9 终端安全

终端安全是企业信息技术安全体系建设的服务对象和密集风险发生部分。我们面临着多方面的挑战，需要采用不同类型，不同层次，不同级别的安全措施，实现终端安全。

9.9.1 挑战和威胁

1. 员工安全意识薄弱，企业安全策略难以实施，网络病毒泛滥

病毒、蠕虫和间谍软件等网络安全威胁损害客户利益并造成大量金钱和生

产率的损失。与此同时，移动设备的普及进一步加剧了威胁。移动用户能够从家里或公共热点连接互联网或办公室网络，常在无意中轻易地感染病毒并将其带进企业环境，进而感染网络。

据 2010 CSI/FBI 安全报告称，虽然安全技术多年来一直在发展，且安全技术的实施更是耗资数百万美元，但病毒、蠕虫和其他形式的恶意软件仍然是各机构现在面临的主要问题。机构每年遭遇的大量安全事故造成系统中断、收入损失、数据损坏或毁坏以及生产率降低等问题，给机构带来了巨大的经济影响。

为了解决这些问题，很多企业都制定了企业的终端安全策略，规定终端必须安装杀毒软件，以及及时更新病毒库；终端必须及时安装系统安全补丁；终端必须设置强口令等。但是由于员工安全意识薄弱，企业的安全策略难以实施，形同虚设，网络安全问题依然严重。

2. 非授权用户接入网络，重要信息泄露

非授权接入包括以下两个部分：

（1）来自外部的非法用户，利用企业管理的漏洞，使用 PC 接入交换机，获得网络访问的权限；然后冒用合法用户的口令以合法身份登录网站后，查看机密信息，修改信息内容及破坏应用系统的运行。

（2）来自内部的合法用户，随意访问网络中的关键资源，获取关键信息用于非法的目的。

目前，企业使用的局域网是以以太网为基础的网络架构，只要插入网络，就能够自由地访问整个网络。因非法接入和非授权访问导致企业业务系统的破坏以及关键信息资产的泄露，已经成为了企业需要解决的重要风险。

3. 网络资源的不合理使用，工作效率下降，存在违反法律法规的风险

根据 IDC 最新数据报导，企事业员工平均每天有超过 50%的上班时间用来在线聊天，浏览娱乐、色情、赌博网站，或处理个人事务；员工从互联网下载各种信息，而在那些用于下载信息的时间中，62%用于软件下载，11%用于下载音乐，只有 25%用于下载与写报告和文件相关的资料。

在国内，法律规定了很多网站是非法的，如有色情内容的、与反政府相关的、与迷信和犯罪相关的等。使用宽带接入互联网后，企事业内部网络某种程度上成了一种“公共”上网场所，很多与法律相违背的行为都有可能发生在内部网络中。这些事情难以追查，给企业带来了法律法规方面的风险。

9.9.2 防护措施

目前，终端数据管理存在的问题主要表现在：数据管理工作难以形成制度化，数据丢失现象时常发生；数据分散在不同的机器、不同的应用上，管理分

散，安全得不到保障；难以实现数据库数据的高效在线备份；存储媒体管理困难，历史数据保留困难。

为此，我们从以下几个方面采取措施实现终端安全。

1．数据备份

随着计算机数据系统建设的深入，数据变得越来越举足轻重，如何有效地管理数据系统日益成为保障系统正常运行的关键环节。然而，数据系统上的数据格式不一，物理位置分布广泛，应用分散，数据量大，造成了数据难以有效的管理，这给日后的工作带来诸多隐患。因此，建立一套制度化的数据备份系统有着非常重要的意义。

数据备份是指通过在数据系统中选定一台机器作为数据备份的管理服务器，在其他机器上安装客户端软件，从而将整个数据系统的数据自动备份到与备份服务器相连的储存设备上，并在备份服务器上为各个备份客户端建立相应的备份数据的索引表，利用索引表自动驱动存储介质来实现数据的自动恢复。若有意外事件发生，若系统崩溃、非法操作等，可利用数据备份系统进行恢复。从可靠性角度考虑，备份数量最好大于等于 2。

1）数据备份的主要内容

（1）跨平台数据备份管理：　要支持各种操作系统和数据库系统；

（2）备份的安全性与可靠性：双重备份保护系统，确保备份数据万无一失；

（3）自动化排程/智能化报警：　通过 Mail/Broadcasting/Log 产生报警；

（4）数据灾难防治与恢复：提供指定目录/单个文件数据恢复。

2）数据备份方案

每个计算环境的规模、体系结构、客户机平台和它支持的应用软件都各不相同，其存储管理需求也会有所区别，所以要选择最适合自身环境的解决方案。目前虽然没有统一的标准，但至少要具有以下功能：集成的客户机代理支持、广泛的存储设备支持、高级介质管理、高级日程安排、数据完整性保证机制、数据库保护。比如，华为公司的 VIS 数据容灾解决方案、HDP 数据连续性保护方案， HDS 的 TrueCopy 方案，IBM 的 SVC 方案等。

2．全面可靠的防病毒体系

计算机病毒的防治要从防毒、查毒、解毒三方面来进行，系统对于计算机病毒的实际防治能力和效果也要从防毒能力、查毒能力和解毒能力三方面来评判。

由于企业数据系统环境非常复杂，它拥有不同的系统和应用。因此，对于整个企业数据系统病毒的防治，要兼顾到各个环节，否则有某些环节存在问题，则很可能造成整体防治的失败。因而，对于反病毒软件来说，需要在技术上做得面面俱到，才能实现全面防毒。

由于数据系统病毒与单机病毒在本质上是相同的，都是人为编制的计算机程序，因此反病毒的原理是一样的，但是由于数据系统具有的特殊复杂性，使

得对数据系统反病毒的要求不仅是防毒、查毒、杀毒，而且还要求做到与系统的无缝链接。因为，这项技术是影响软件运行效率、全面查杀病毒的关键所在。但是要做到无缝链接，必须充分掌握系统的底层协议和接口规范。

随着当代病毒技术的发展，病毒已经能够紧密地嵌入操作系统的深层，甚至是内核之中。这种深层次的嵌入，为彻底杀除病毒造成了极大的困难，如果不能确保在病毒被杀除的同时不破坏操作系统本身，那么，使用这种反病毒软件也许会出现事与愿违的严重后果。无缝链接技术可以保证反病毒模块从底层内核与各种操作系统、数据系统、硬件、应用环境密切协调，确保在病毒入侵时，反病毒操作不会伤及操作系统内核，同时又能确保对来犯病毒的防杀。

VxD 是微软专门为 Windows 制定的设备驱动程序接口规范。简而言之，VxD 程序有点类似于 DOS 中的设备驱动程序，它是专门用于管理系统所加载的各种设备。VxD 不仅适用于硬件设备，而且由于它具有比其他类型应用程序更高的优先级，更靠近系统底层资源，因此，在 Windows 操作系统下，反病毒技术就需要利用 VxD 机制才有可能全面、彻底地控制系统资源，并在病毒入侵时及时报警。而且，VxD 技术与 TSR 技术有很大的不同，占用极少的内存，对系统性能影响极小。

由于病毒具备隐蔽性，因此它会在不知不觉中潜入你的机器。如果不能抵御这种隐蔽性，那么反病毒软件就谈不上防毒功能了。实时反病毒软件作为一个任务，对进出计算机系统的数据进行监控，能够保证系统不受病毒侵害。同时，用户的其他应用程序可作为其他任务在系统中并行运行，与实时反病毒任务毫不冲突。因此，在 Windows 环境下，如果不能实现实时反病毒，那么也将会为病毒入侵埋下隐患。针对这一特性，需要采取实时反病毒技术，保证在计算机系统的整个工作过程中，能够随时防止病毒从外界入侵系统，从而全面提高计算机系统的整体防护水平。

当前，大多数光盘上存放的文件和数据系统上传输的文件都是以压缩形式存放的，而且情况很复杂。现行通用的压缩格式较多，有的压缩工具还将压缩文件打包成一个扩展名为“.exe”的“自解压”可执行文件，这种自解压文件可脱离压缩工具直接运行。对于这些压缩文件存在的复杂情况，如果反病毒软件不能准确判断，或判断片面，那就不可避免地会留有查杀病毒的“死角”，为病毒防治造成隐患。可通过全面掌握通用压缩算法和软件生产厂商自定义的压缩算法，深入分析压缩文件的数据内容，而非采用简单地检查扩展文件名的方法，实现对所有压缩文件的查毒杀毒功能。

对于数据系统病毒的防治来说，反病毒软件要能够做到全方位的防护，才能对病毒做到密而不漏的查杀。对于数据系统病毒，除了对软盘、光盘等病毒感染最普遍的媒介具备保护功能外，对于更为隐性的企业数据系统传播途径，更应该把好关口。

当前，公司之间以及人与人之间电子通信方式的应用更为广泛。但是，随着这种数据交换的增多，越来越多的病毒隐藏在邮件附件和数据库文件中进行

传播扩散。因此，反病毒软件应该对这一病毒传播通道具备有效控制的功能。

伴随数据系统的发展，在下载文件时，被感染病毒的机率正在呈指数级增长。对这一传播更为广泛的病毒源，需要在下载文件中的病毒感染机器之前，自动将之检测出来并给予清除，对压缩文件同样有效。

简言之，要综合采用数字免疫系统、监控病毒源技术、主动内核技术、“分布式处理”技术、安全网管技术等措施，提高系统的抗病毒能力。

3．安全措施之防火墙及数据加密

所谓防火墙就是一个把互联网与内部网隔开的屏障。防火墙有两类，即标准防火墙和双家网关。随着防火墙技术的进步，在双家网关的基础上又演化出两种防火墙配置，一种是隐蔽主机网关，另一种是隐蔽智能网关（隐蔽子网）。隐蔽主机网关是当前一种常见的防火墙配置。顾名思义，这种配置一方面将路由器进行隐蔽，另一方面在互联网和内部网之间安装堡垒主机。堡垒主机装在内部网上，通过路由器的配置,使该堡垒主机成为内部网与互联网进行通信的唯一系统。目前技术最为复杂而且安全级别最高的防火墙是隐蔽智能网关，它将网关隐藏在公共系统之后使其免遭直接攻击。隐蔽智能网关提供了对互联网服务进行几乎透明的访问，同时阻止了外部未授权访问者对专用数据系统的非法访问。一般来说，这种防火墙是最不容易被破坏的。

与防火墙配合使用的安全技术还有数据加密技术，是为提高信息系统及数据的安全性和保密性，防止秘密数据被外部破析所采用的主要技术手段之一。随着信息技术的发展，数据系统安全与信息保密日益引起人们的关注。目前各国除了从法律上、管理上加强数据的安全保护外，从技术上分别在软件和硬件两方面采取措施，推动着数据加密技术和物理防范技术的不断发展。按作用不同，数据加密技术主要分为数据传输、数据存储、数据完整性的鉴别以及密钥管理技术四种。

4．智能卡实施

与数据加密技术紧密相关的另一项技术则是智能卡技术。所谓智能卡就是密钥的一种媒体，一般就像信用卡一样，由授权用户所持有并由该用户赋予它一个口令或密码字。该密码与内部数据系统服务器上注册的密码一致。当口令与身份特征共同使用时，智能卡的保密性能还是相当有效的。数据系统安全和数据保护的这些防范措施都有一定的限度，并不是越安全就越可靠。因而，在看一个内部网是否安全时不仅要考察其手段，而更重要的是对该数据系统所采取的各种措施，其中不光是物理防范，还有人员的素质等其他“软”因素，进行综合评估，从而得出是否安全的结论。

另外，其他具体安全措施还包括数字认证、严谨有效的管理制度和高度警惕的安全意识以及多级网管等措施。另外考虑到数据系统的业务连续，也需要我们设计和部署必要的 BCP 计划。

9.9.3 解决方案

解决终端安全问题的有效方法是结合端点安全状况信息和新型的网络准入控制技术。

（1）部署和实施网络准入控制，通过准入控制设备，能够有效地防范来自非法终端对网络业务资源的访问，有效防范信息泄密。

（2）通过准入控制设备，实现最小授权的访问控制，使得不同身份和角色的员工，只能访问特定授权的业务系统，保护如财务系统企业的关键业务资源。

（3）端点安全状态与网络准入控制技术相结合，阻止不安全的终端以及不满足企业安全策略的终端接入网络，通过技术的手段强制实施企业的安全策略，来减少网络安全事件，增强对企业安全制度的遵从。

加强事后审计，记录和控制终端对网络的访问，控制网络应用程序的使用，敦促员工专注工作，减少企业在互联网访问的法律法规方面的风险，并且提供责任回溯的手段。

1. 集中式组网方案

终端安全管理（Terminal Security Management，TSM）系统支持集中式组网，把所有的控制服务器集中在一起，为网络中的终端提供接入控制和安全管理功能。集中式组网方案如图 9-3 所示。

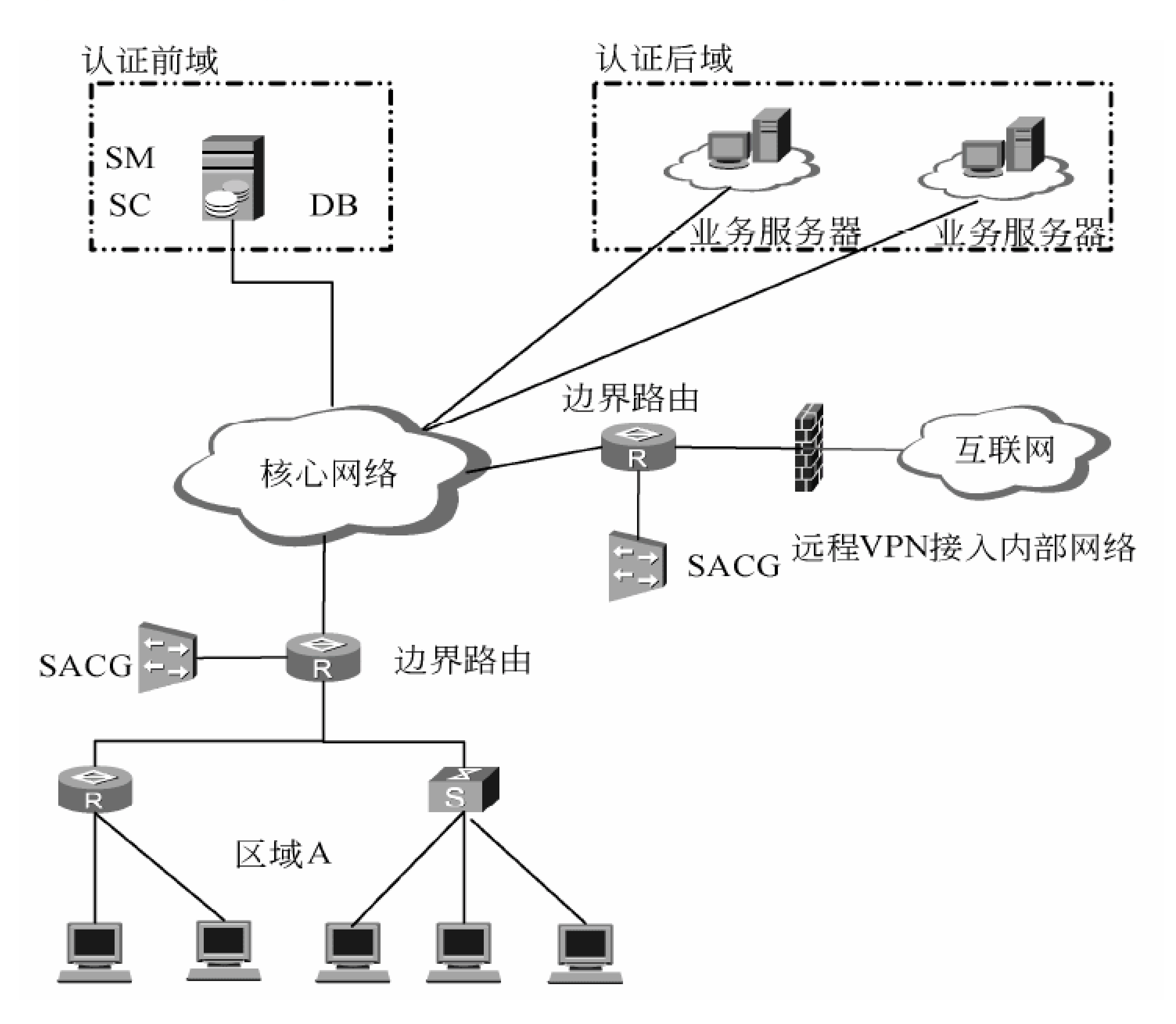


图 9-3　集中式组网逻辑示意图

2. 分布式组网方案

如果遇到下面的情况，可能需要采用分布式组网方案，如图 9-4 所示。

（1）终端相对集中在几个区域，而且区域之间的带宽比较小，由于代理与服务器之间存在一定的流量，如果采用集中式部署，将会占用区域之间的带宽，影响业务的提供。

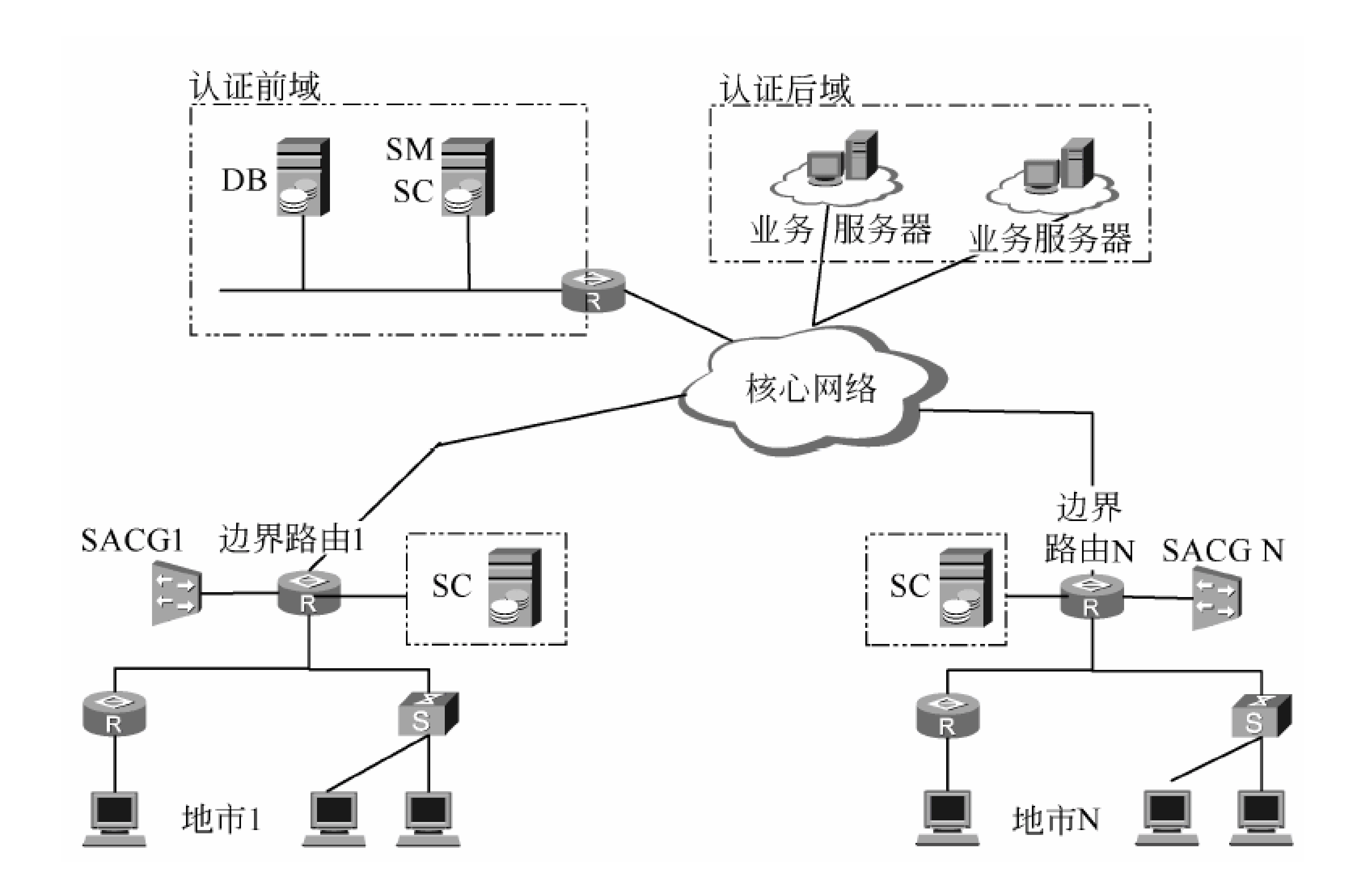


图 9-4　分布式组网方案

（2）终端的规模相当大，可以考虑使用分布式组网，避免大量终端访问 TSM 服务器，占用大量的网络带宽。

分布式部署的时候，TSM 安全代理选择就近的控制服务器，获得身份认证和准入控制等各项业务。

3．分级式组网方案

如果网络规模超大，可以选择采用分级式组网方案，如图 9-5 所示。

在这种部署方案中，每个 TSM 结点都是一个独立的管理单元，承担独立的用户管理、准入控制以及安全策略管理业务。管理中心负责制定总体的安全策略，下发给各个 TSM 管理结点，并且对 TSM 管理结点实施情况进行监控。

TSM 系统对于关键的用户认证数据库提供镜像备份机制，当主数据库发生故障时，镜像数据库提供了备份的认证源，能够保证基本业务的提供，防止因为单一数据源失效导致接入控制的网络故障。

当 TSM 系统发生严重故障，或者 TSM 系统所在的网络发生严重故障时，用户可以根据业务的情况进行选择：业务优先/安全优先。

如果选择业务优先，准入控制设备（802.1x 交换机除外）上设计的逃生通道能够检测到 TSM 系统的严重故障，启用逃生通道，防止重要业务中断。

TSM 终端安全管理系统提供服务器状态监控工具，通过该工具可以监控服务器的运行状态，如数据库链接不上、SACG 链接故障以及 CPU/内存异常等。当检查到服务器的状态异常时，可以通过邮件、短信等方式通知管理员及时处理。

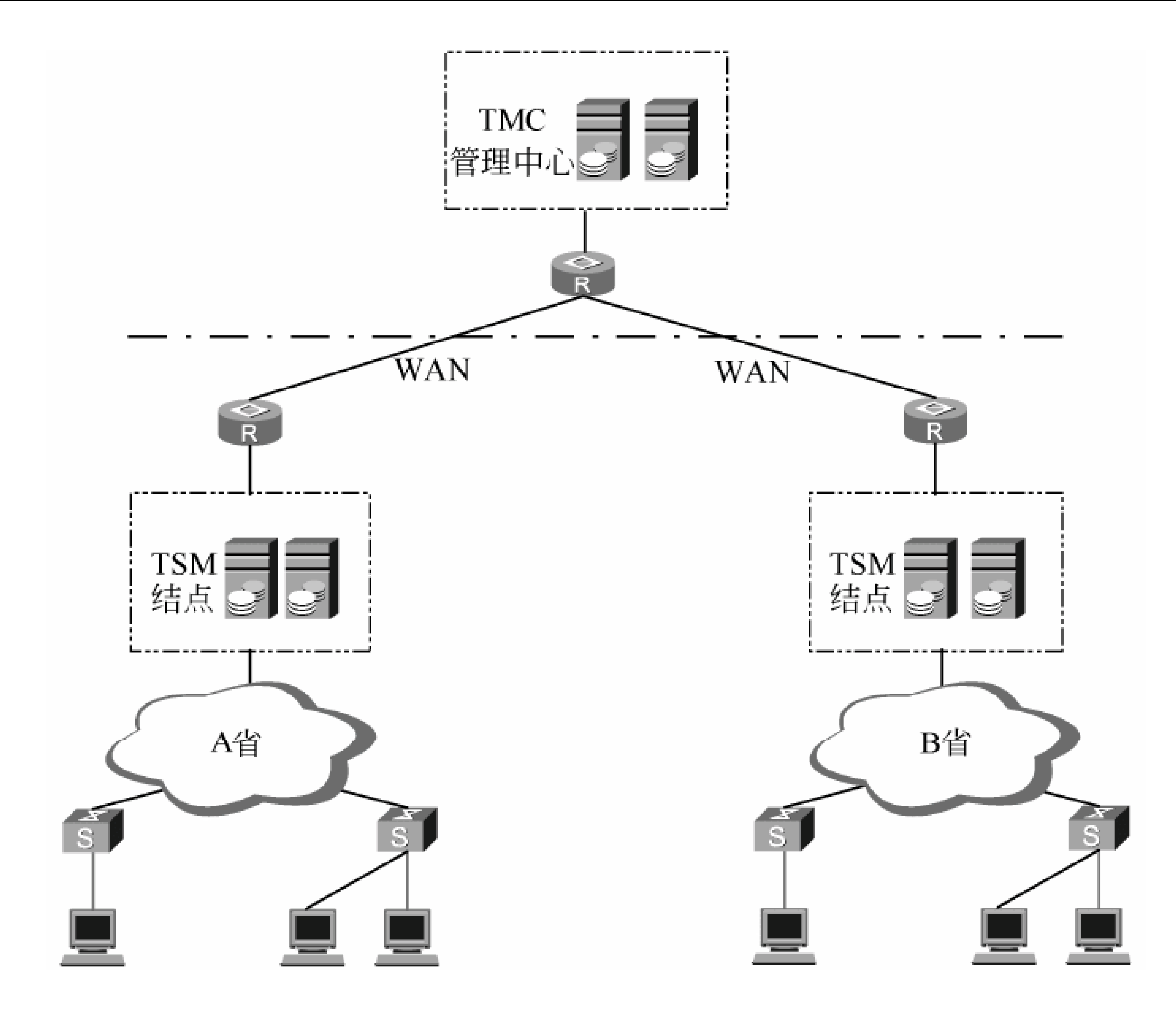


图 9-5 分级式组网方案

9.9.4 终端虚拟化技术

1. 传统的终端数据安全保护技术

1）DLP

（1）工作方式：DLP（Data Loss Prevention，数据丢失防护）技术侧重于信息泄密途径的防护，是能够通过深度内容分析对动态数据、静态数据和使用中的数据进行鉴定、检测和保护的产品。可以在 PC 终端、网络、邮件服务器等系统上针对信息内容层面的检测和防护，能够发现你的敏感数据存储的位置，之后进行一定的处理方式，但也是有些漏洞的。

（2）使用场景与限制：虽然 DLP 方案从灵活性、安全性、管理性上都满足了数据安全的需求，但同样成功部署 DLP 方案需要有一个前提，就是其数据内容匹配算法的误报率要足够低。然而，由于数据内容的表达方式千差万别，在定义数据内容匹配规则的时候漏审率和误判率非常难平衡，无论是哪个厂商的 DLP 产品，在实际测试过程中的误报率普遍都偏高，DLP 方案的防护效果体验并不好。

2）DRM

（1）工作方式：DRM（Digital Right Management，数字权限管理）是加密及元数据的结合，用于说明获准访问数据的用户，以及他们可以或不可以对数据运行进行某些操作。DRM 可决定数据的访问及使用方式，相当于随数据一起移动的贴身保镖。权限包括读取、更改、剪切/粘贴、提交电子邮件、复制、

移动、保存到便携式保存设备及打印等操作。虽然 DRM 的功能非常强大，但难以大规模实施。

（2）使用场景与限制：DRM 极其依赖手动运行，因此难以大规模实施。用户必须了解哪些权限适用于哪种内容的用户，这样的复杂程度常使得员工忽略 DRM，并导致未能改善安全性的失败项目。如同加密一样，企业在应用权限时必须依赖人为的判断，因为 DRM 工具不具备了解内容的功能。成功的 DRM 部署通常只限于用户训练有素的小型工作组。由于存在此种复杂性，大型企业通常并不适合部署 DRM。但如同加密一样，可以使用 DLP 来专注于 DRM，并减少某些阻碍广泛部署的手动进程。

3）全盘加密

（1）工作方式：所谓全盘加密技术，一般是采用磁盘级动态加解密技术，通过拦截操作系统或应用软件对磁盘数据的读/写请求，实现对全盘数据的实时加解密，从而保护磁盘中所有文件的存储和使用安全，避免因便携终端或移动设备丢失、存储设备报废和维修所带来的数据泄密风险。

（2）使用场景与限制：与防水墙技术类似，全盘加密技术还是无法对不同的涉密系统数据进行区别对待，不管是涉密文件还是普通文件，都进行加密存储，无法支持正常的内外部文件交流。另外，全盘加密方案虽然能够从数据源头上保障数据内容的安全性，但无法保障其自身的安全性和可靠性，一旦软件系统损坏，所有的数据都将无法正常访问，对业务数据的可用性而言反而是一种潜在的威胁。

上述传统安全技术是目前银行业都会部署的基础安全系统，这些安全系统能够在某一个点上起到防护作用，然而尽管如此，数据泄密事件依然是屡禁不止，可见银行业网络整体安全目前最大的威胁来源于终端安全上。而且部署这么多的系统方案以后，用户体验不佳，不容易推广，因此并未达到预期的效果。要彻底改变企业内网安全现状，必须部署更为有效的涉密系统数据防泄密方案。

2. 数据保护的创新——终端虚拟化技术

为了能够在确保数据安全的前提下，提升用户的易用性和部署快速性，目前已经有部分企业开始使用终端虚拟化的技术来实现数据安全的保护。其中，桌面/应用虚拟化技术以及基于安全沙盒技术的虚拟安全桌面就是两种比较常见的方式。

1）桌面/应用虚拟化

桌面/应用虚拟化技术是基于服务器的计算模型，它将所有桌面虚拟机在数据中心进行托管并统一管理。通过采购大量服务器，将 CPU、存储器等硬件资源进行集中建设，构建一个终端服务层，从而将桌面、应用以图像的方式发布给终端用户。作为云计算的一种方式，由于所有的计算都放在服务器上，对终端设备的要求将大大降低，不需要传统的台式计算机、笔记本式计算机，用户可以通过客户端或者远程访问等方式获得与传统 PC 一致的用户体验，如图 9-6 所示。

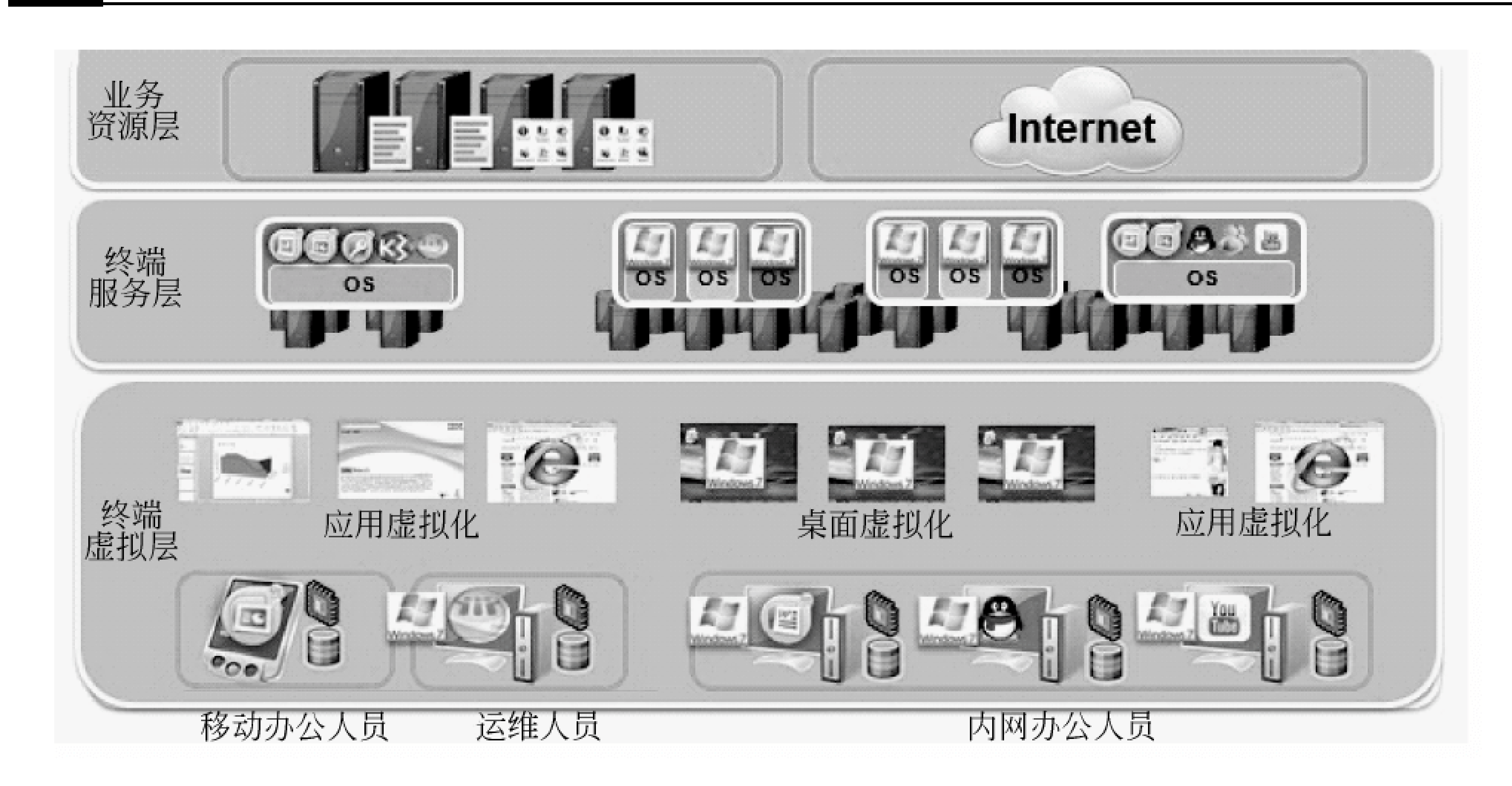


图 9-6 桌面虚拟化

不过，虽然基于计算集中化模式的桌面虚拟化技术能够大大简化终端的管理维护工作，能够很好地解决终端数据安全问题，但是也带来了服务端的部署成本过大和管理成本提高等新问题。

（1）所有的客户端程序进程都运行在终端服务器上，需要配置高性能的终端服务器集群来均衡服务器的负载压力。

（2）由于网络延迟、服务器性能、并发拥塞等客观因素影响，在桌面虚拟化方案中，终端用户的使用体验大大低于物理计算机本地应用程序的使用体验。

（3）计算集中化容易带来终端服务器的单点故障问题，需要通过终端服务器的冗余备份来强化系统的稳定性。

（4）桌面虚拟化方案中部署的大量终端服务器以及集中化的数据存储之间的备份、恢复、迁移、维护、隔离等问题。

（5）由于数据集中化，管理员的权限管理也需要列入考虑，毕竟让网络管理员能够接触到银行业务部门的业务数据也是违背数据安全需求的。

（6）桌面集中化方案提高了对网络的稳定性要求，无法满足离线办公的需求。

因此，此种方案在大规模部署使用时会遇到成本高、体验差的问题，如图 9-7 所示。

2）防泄密安全桌面

为了解决桌面/应用虚拟化存在的问题，一种新的终端虚拟化技术——基于沙盒的安全桌面被应用到了防泄密领域，如图 9-8 所示。

在不改变当前 IT 架构的情况下，充分利用本地 PC 的软、硬件资源，在本地直接通过安全沙盒技术虚拟化了一个安全桌面，这个桌面可以理解为原有默认桌面的一个备份和镜像，在安全桌面环境下运行的应用、数据、网络权限等完全与默认桌面隔离，并且安全沙盒可以针对不同桌面之间进行细粒度的安全控制，比如安全桌面下只能访问敏感业务系统，安全桌面内数据无法外发、复制、打印、截屏，安全桌面内保存的文件加密存储等等。

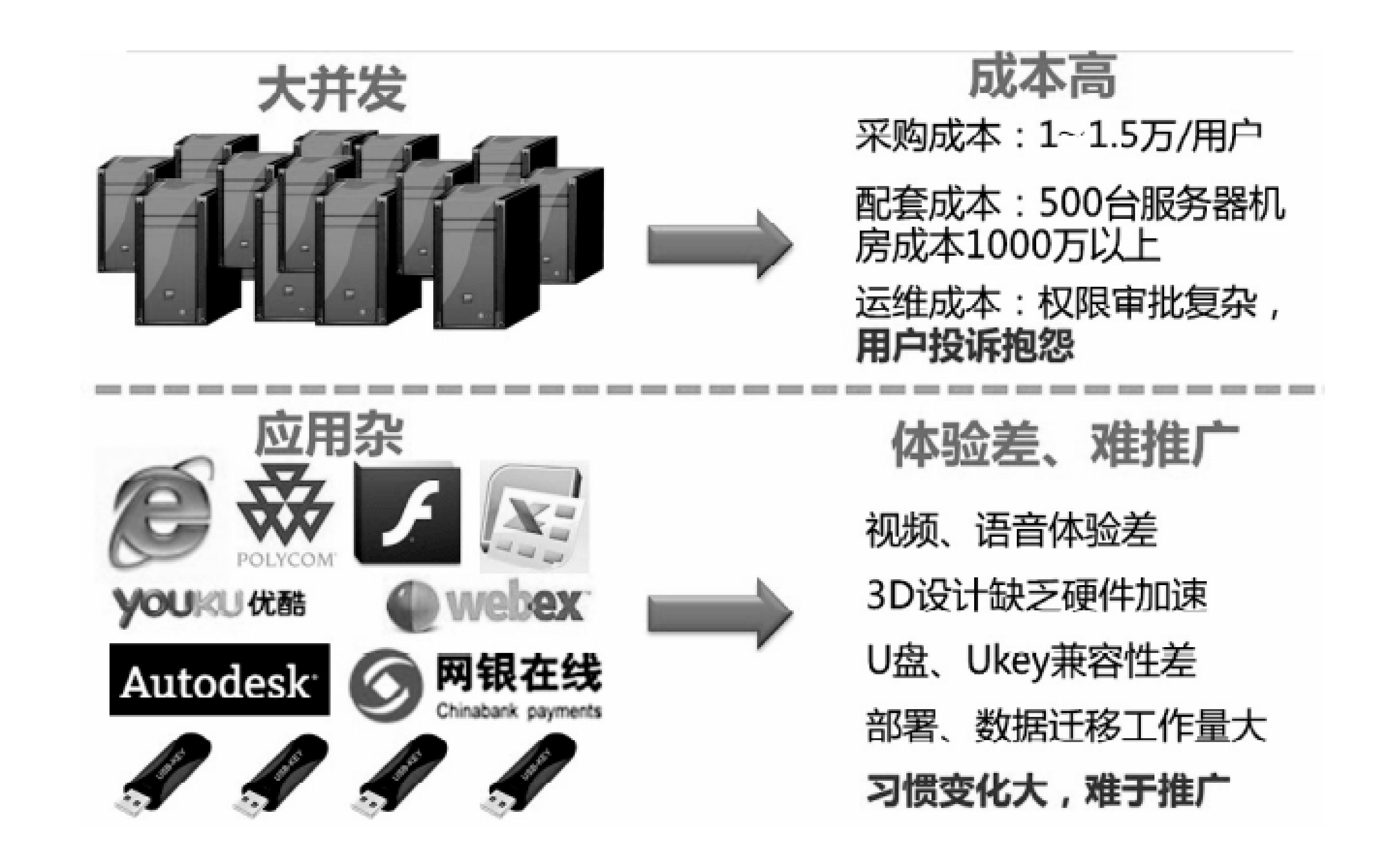


图 9-7　桌面虚拟化带来的问题

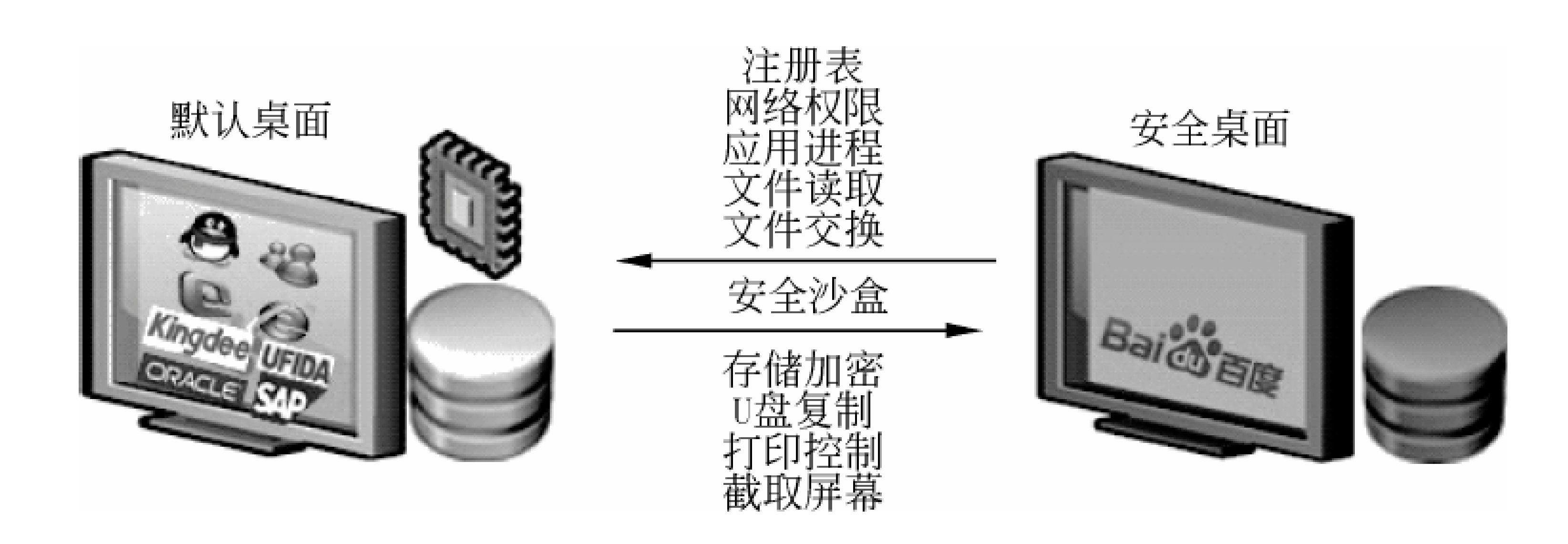


图 9-8　基于沙盒的安全桌面

这样一来，通过安全桌面+安全控制网关的联通配合，就可以确保用户只有在防泄密安全桌面内进行了认证后才能访问核心敏感系统，实现了在终端的多业务风险隔离，确保了终端的安全性。安全桌面虚拟化方案为用户提供了多个虚拟的安全桌面，通过不同虚拟安全桌面相互隔离文件资源、网络资源、系统资源等，可以让用户通过不同的桌面访问不同的业务资源。

比如为用户访问涉密业务系统提供了一个具有数据防泄露防护的防泄密安全桌面，尽可能减少对用户使用习惯的影响，解决了物理隔离方案的易用性问题，如图 9-9 所示。

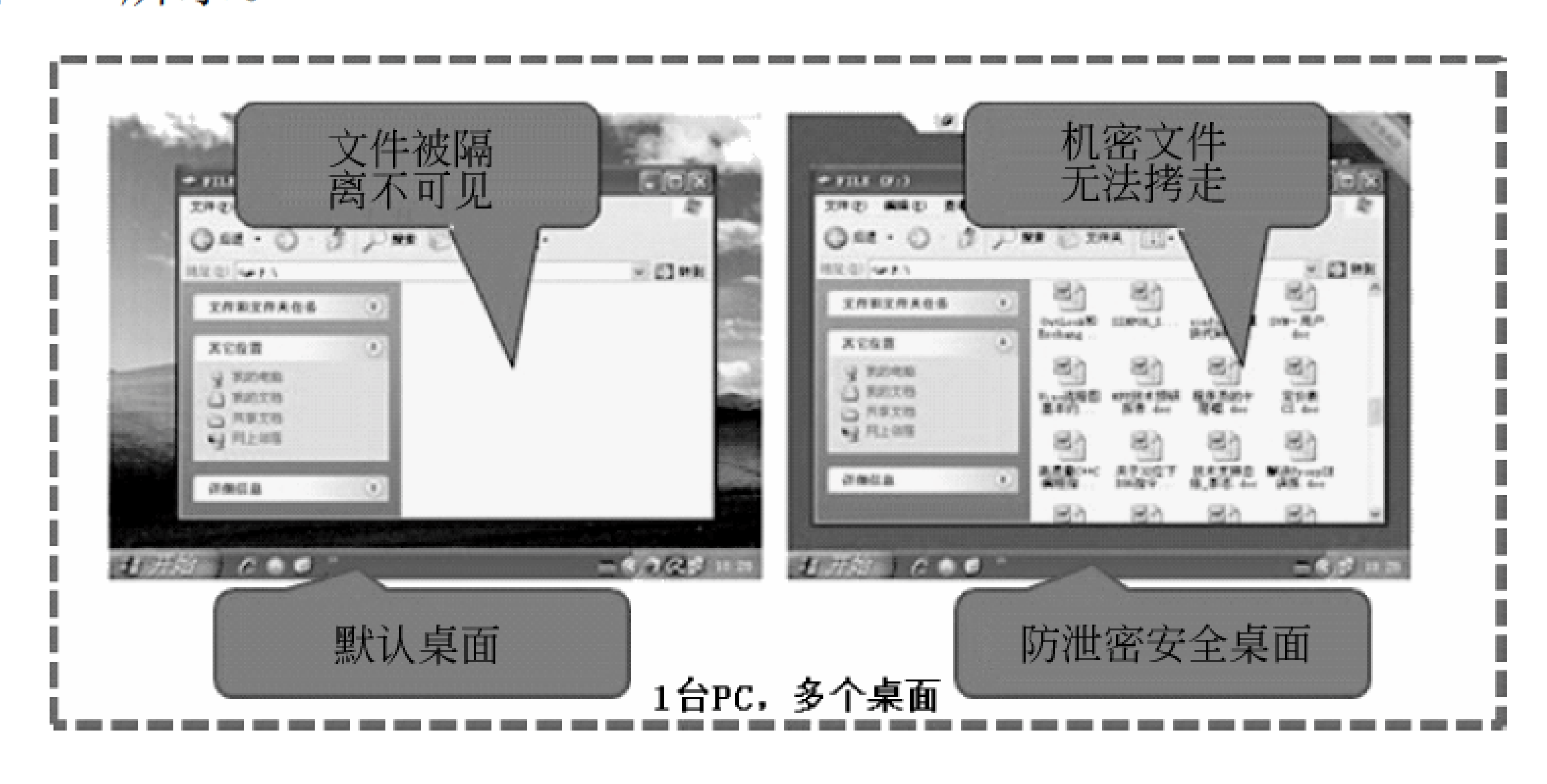


图 9-9　多个桌面

基于沙盒的安全桌面方案的价值在于，在实现终端敏感业务数据防泄密的前提下，不改变用户使用习惯，增强了易用性，还保护了用户的现有投资。目前，防泄密安全桌面已经在金融、政府、企业等单位开始了广泛的应用，主要部署在 CRM、ERP、设计图样等系统前端，以防止内部销售、供应链、财务等人员的主动泄密行为。

但是安全桌面技术也有一定的局限性，比如它不适用于 Java、C 语言的代码开发环境，存在一定兼容性的问题。

总而言之，两种终端虚拟化技术各有优劣，分别适用于不同的业务场景，具体可以参照图 9-10。

业务场景	普通员工日常业务	开发设计部门	IT 后台运维业务	客户服务呼叫中心部门
使用规模	规模大、并发高内部员工	规模中等、并发高	规模小、并发低 IT 部门、第三方合作伙伴	规模中等 并发高
人员 IT 技术水平	层次不齐，大部分具备初级能力	水平较高，懂得编程开发	水平较高，懂得编程开发，有管理权限	层次不齐，大部分具备初级能力
安全风险级别，泄密手段	泄密手段简单，安全风险中等	泄密手段多样，安全风险高	泄密手段多样，安全风险高	泄密手段简单，安全风险中等
用户个性化要求和复杂度	个性化需求较多 私人数据量较多 兼容性要求高	个性化需求较少 私人数据量较少	个性化需求较少 私人数据量较少	个性化需求较多 私人数据量较多 兼容性要求高
建议方案	安全桌面	安全桌面	桌面/应用虚拟化	安全桌面

图 9-10　不同桌面虚拟化的比较

9.9.5　安全沙盒虚拟隔离技术

目前，内网 PC 在访问互联网的过程中经常会感染木马、病毒、蠕虫，会给企业内网带来极大的危害。比如，病毒/蠕虫可以在内网大规模传播导致网络中断，木马入侵 PC 后会扫描主机上的敏感信息/个人信息外发，病毒感染 PC 后的运维工作量也会急剧提升等。因此，目前主要的主机防病毒/木马技术分为主机反病毒保护和安全沙盒虚拟隔离两种，这两种技术应该相辅相成配合使用以具备更好的主机反病毒效果。

1. 反病毒软件技术

反病毒软件的任务是实时监控和扫描主机的磁盘、进程，防止病毒感染主机。反病毒软件的实时监控方式因软件而异。

（1）特征比对式：通过在内存里划分一部分空间，将计算机里流过内存的数据与反病毒软件自身所带的病毒库（包含病毒定义）的特征码相比较，以判

断是否为病毒。其优点是精确度高，缺点是存在滞后性，针对最新的病毒需要不断更新特征。

（2）虚拟机式：随着病毒技术的发展，加密技术渐渐成熟起来，很多病毒的特征都不再那么容易提取。这样，虚拟机杀毒技术出现了。所谓虚拟机技术，就是用软件先虚拟一套运行环境，让病毒先在该虚拟环境下运行，看看它的执行效果。由于加密的病毒在执行时最终还是要解密的，这样，在其解密之后我们可以通过特征值查毒法对其进行查杀。但是虚拟机技术的问题就是效率问题，会较大程度地影响用户的使用速度。

（3）启发式：新病毒不断出现，传统的特征值查毒法完全不可能查出新出现的病毒。这样，启发式扫描技术产生了，何谓启发式扫描？我们知道，一个病毒总存在与普通程序不一般的地方，譬如它会格式化硬盘、重定位、改回文件时间、修改文件大小、能够传染等等。这样，我们就可以对每一类病毒特征进行加权，譬如重定位 3 分，格式化硬盘 15 分，传染 10 分，如果一个程序拥有这三个功能，它就得到了 28 分，如果我们设定判断一个病毒的标准是 20 分，那么这个程序在遇到采用了启发式扫描技术的杀毒软件时，杀毒软件就会报警，说发现新病毒。但是启发式技术也存在着一定的问题，比如检测精度无法实现 100%的有效性、检测效率有待提升等。

因此，我们可以看出无论是哪种反病毒技术，都有一定优缺点，用户应该根据自己 IT 系统的特点选择部署。

2. 反病毒的创新——安全沙盒虚拟隔离技术

安全沙盒技术的诞生给主机反病毒提供了一个新的解决思路，那就是在主机上提供一个虚拟桌面环境，其与本地默认桌面环境相隔离，让用户在进行访问互联网等存在引入病毒风险可能性的行为时，必须在虚拟桌面下进行，一旦感染了病毒木马不会对默认桌面产生影响，只需要重启虚拟桌面环境，就能够自动清除病毒，快速恢复一个干净的、与默认桌面一样的新的虚拟环境，如图 9-11 所示。

安全沙盒技术让这种解决思路成为了可能：首先，安全沙盒是一个轻量级的虚拟化技术，只需要占用 10%的 CPU 利用率，100MB 左右的内存，开启/恢复迅速，只需要 10～20s 时间，不会影响主机运行速度；其次，安全沙盒虚拟的桌面与默认系统一致，从桌面壁纸到应用程序等都可以平滑使用，不会让用户的使用体验有较大变化；最后，安全沙盒安全隔离控制粒度较细，可以提供网络权限、磁盘访问、注册表、内存访问等多个层面的安全隔离，从而确保病毒不会感染默认系统。

目前，主流的安全沙盒虚拟隔离技术往往采用与网关配合的方式进行联动部署。上网安全桌面可以与上网行为管理设备配合，只允许在上网安全桌面环境下才能访问互联网，从而实现了互联网与内网 PC 的隔离，避免互联网病毒等风险感染内网 PC 和网络，如图 9-12 所示。



图 9-11　反病毒的创新—安全沙盒虚拟隔离技术

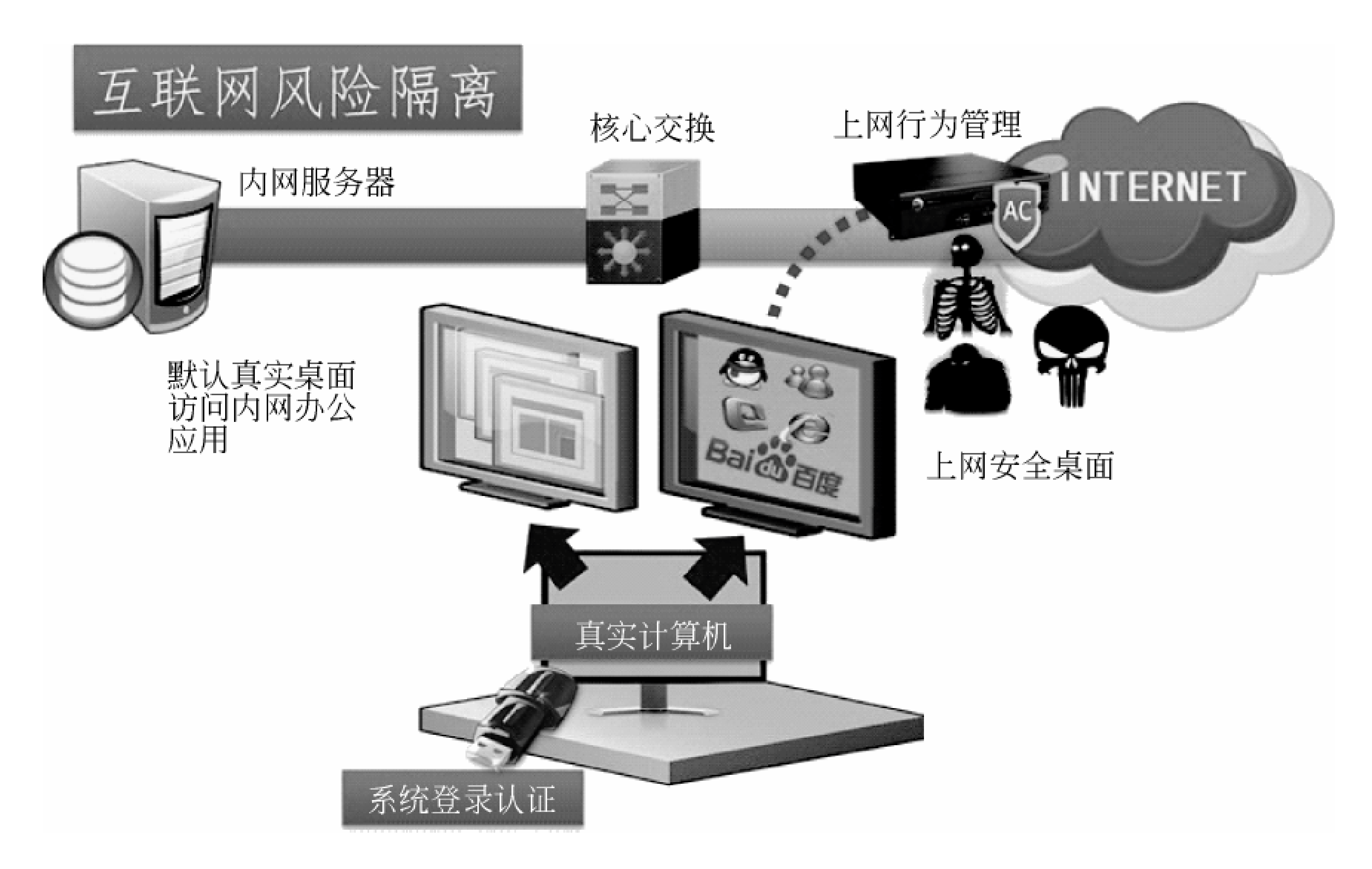


图 9-12　安全沙盒虚拟隔离技术

第10章 信息安全体系建设

企业信息安全框架的设计与确定是指导企业进行信息安全体系建设的基本依据，前面章节论述了企业信息安全框架的概念、设计原则、主要内容等，本章以企业信息安全框架为指导，提出企业信息安全体系建设的基本策略和方法。

10.1 信息安全体系建设策略

企业信息安全体系建设是企业信息化建设中的重要组成部分，为企业业务规范管理、经营效益、社会效益等诸多方面提供基本保障。

本书所描述的企业信息安全框架参考了信息安全理论、标准以及众多企业所积累的经验，充分吸取行业中的最佳实践。在具体运用中可结合信息安全的相关方法论、模型及标准，将所有的内容与要求基于企业的业务需求和现状，转化到信息安全设计与规划的具体项目中分别予以实现，并提供可参照执行的演进路径。从企业战略、实际需求出发，参照企业信息安全管理框架，通过评估和风险分析等方法，定义企业的安全需求，根据企业的安全需求定义企业信息安全建设的内容和方向。为了保障企业的信息安全，必须建立一个信息安全体系。信息安全体系包含信息安全管理、信息安全技术和信息安全运维三部分内容，三者既有机结合又相互支撑，如图 10-1 所示。企业的信息安全体系运作就是企业根据安全策略，由安全组织（或人员）以安全技术作为工具和手段进行操作，来维持企业网络的安全运行，从而使网络安全可靠。

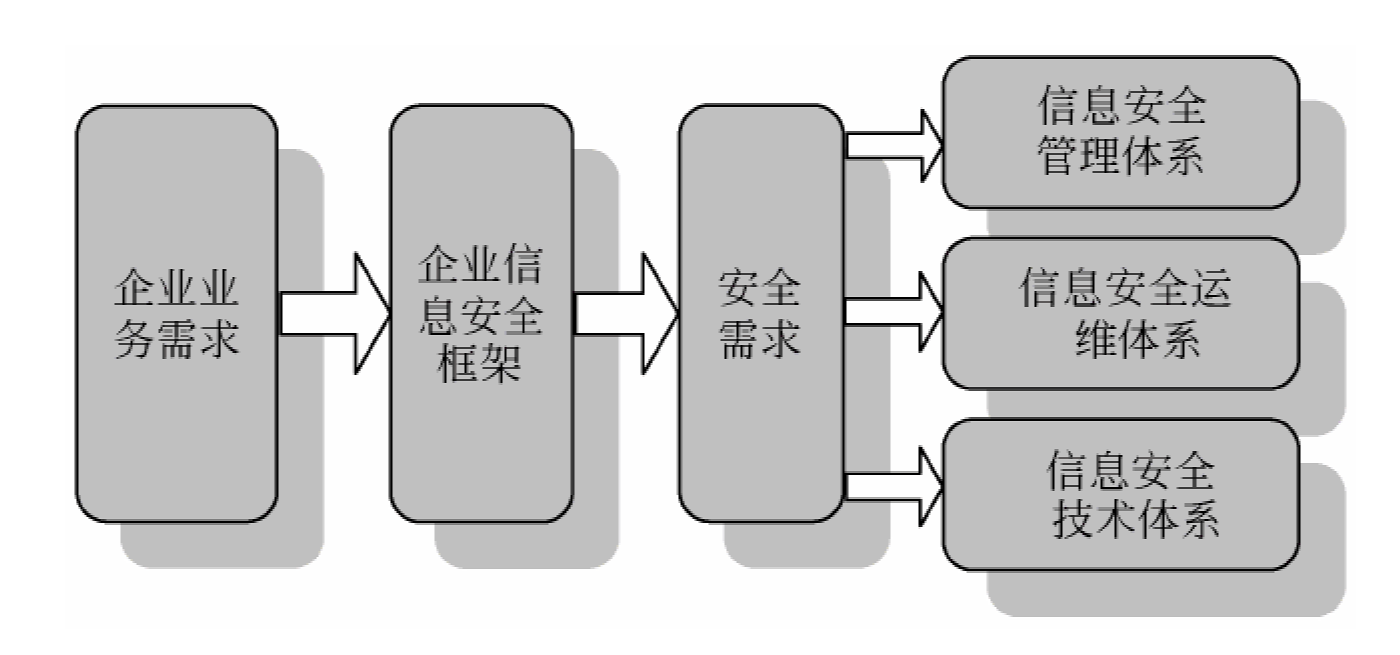


图 10-1 企业信息安全体系建设策略

10.1.1 信息安全建设原则

信息安全体系的建设，涉及面广、工作量大，必须坚持以下的原则，保证建设和运营的效果。

1．统一规划

要对信息安全体系建设进行统一的规划，制定信息安全体系框架，明确保障体系中所包含的内容。同时，还要制定统一的信息安全建设标准和管理规范，使得信息安全体系建设能够遵循一致的标准，管理能够遵循一致的规范。

2．分步有序实施

信息安全体系的建设，内容庞杂，必须坚持分步骤的有序实施原则，循序渐进地进行。

3．技术管理并重

仅有全面的安全技术和机制是远远不够的，安全管理也具有同样的重要性，企业信息安全体系的建设，必须遵循安全技术和安全管理并重的原则，制定统一的安全建设管理规范，指导安全管理工作。

10.1.2 信息安全建设策略方法

无论是 BS 7799 标准中所强调的 PDCA（Plan-Do-Check-Action）流程，还是流行的信息安全方法论所强调的评估、计划、设计、执行与营运等各步骤，要做好信息安全都是必须要先确认企业的业务战略目标与信息安全需求，而未来所导入的任何解决方案均应符合目标与需求。那么如何起步呢？使用成熟度评估模型，跨越所有的信息安全领域去了解您的安全状况，在安全性与投资之间找到均衡点，开发有先后之分的安全路线图。

1．信息安全框架导入

导入信息安全框架，大致包含了信息安全管理体系和 IT 解决方案等建设。一般而言，在时间许可的前提之下，按部就班的从风险评估开始做起，先了解企业所面临的安全威胁，以及可能造成的伤害之后，按照影响程度，配合适当的效益分析，依序根据预算与急迫程度执行解决方案，以降低风险，是最为理想的策略。但在现实中，企业常常面临时间、预算，甚至于来自客户、供应商等方面的业务压力，而无法按照上述的方式执行，必须在短时间内针对急迫的问题迅速拟定执行解决方案，结果容易使得导入的解决方案只能治标，或是缺乏扩充的弹性，而无法面对未来变化的环境。

因此，对于一个组织在导入信息安全框架时，建议采用图 10-2 所示的方法、

步骤及内容。

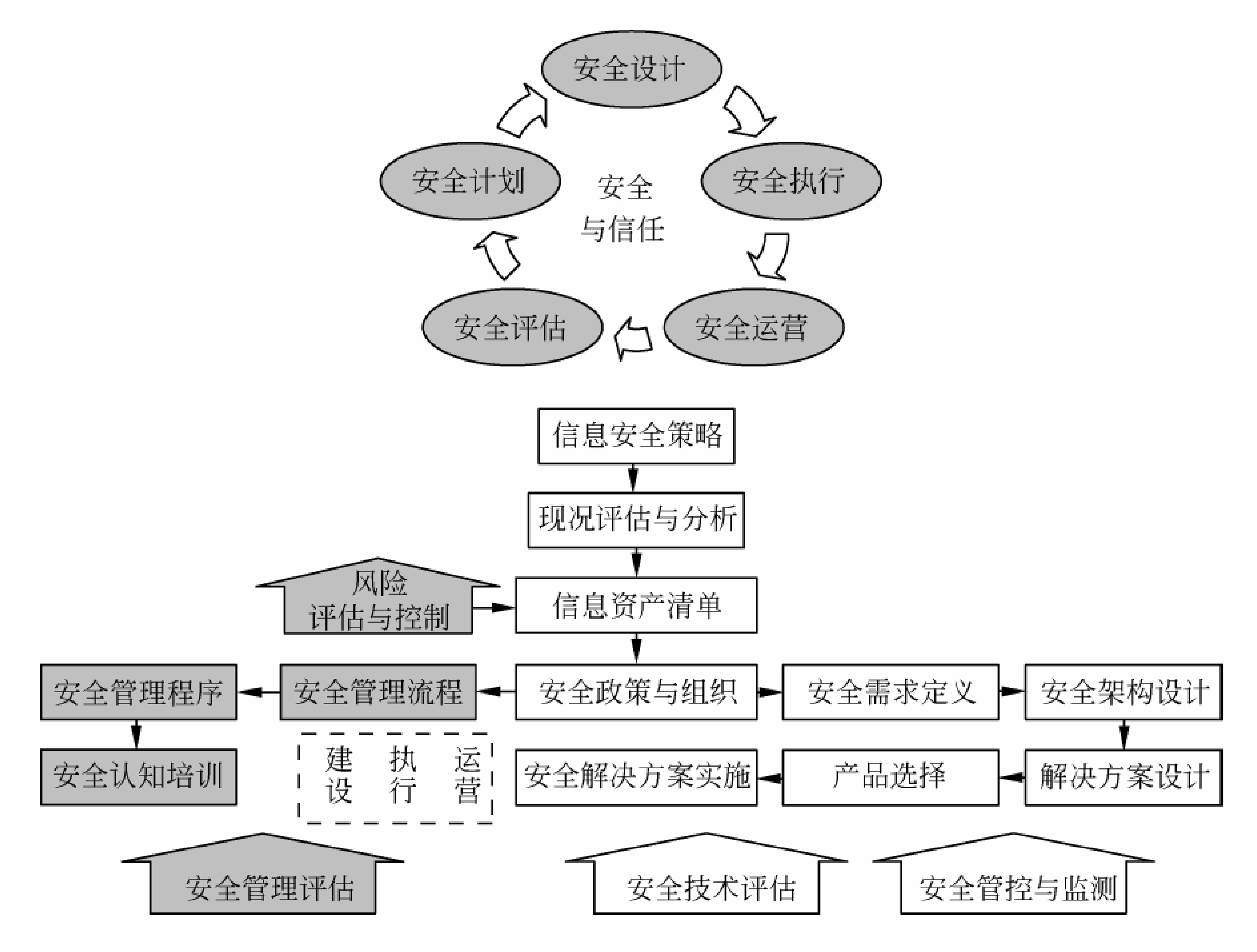


图 10-2 信息安全框架建设导入方法步骤

1）信息安全策略

信息安全所涵盖的范围极为广泛，而要做到百分之百的安全，事实上是几乎不可能的，而且会耗用极大的资源。重要的是必须根据不同行业的特性来规划，例如，高科技产业通常着重于保障先进研发成果数据的机密，而重要民生系统则必须维持系统的运作不致中断等，不同企业在信息安全上的实施策略均不相同。由高层管理人员依照战略目标与核心竞争力提升来考虑制定信息安全策略，引导实际实施的走向，会是较为可行的做法。

2）现况评估与分析

大部分企业均已实施一些信息安全的措施与技术。然而，目前所缺乏的是具备一套有效的系统方法，以便了解本身的信息安全缺失，以及现有的信息安全措施与技术是否能提供足够的防御保障。所以现况的评估与分析极为重要，安全顾问可借助访谈、文件收集、现场调研等不同手段，收集企业目前的实施状况信息，除了可以进一步分析企业的信息安全状况外，还可以了解企业文化，为未来在修订信息安全措施或引进新的信息安全技术时，配合企业的文化拟定切实可行的方案。

3）信息资产清单

实施信息安全也是为了保障企业信息资产的安全。因此，了解公司拥有哪些信息资产是当务之急。企业各部门应列出其负责与拥有的信息资产清单，并

评估其受到损害时对企业所造成的损失及影响，从而进一步了解各项信息资产对公司的重要性。除了列出清单之外，针对每项资产，也应当进行风险评估，以了解这些信息资产可能面临的问题，以及问题发生时对公司的伤害程度，如图 10-3 所示的流程。

风险评估乃是根据资产的价值，以及该资产所面临的威胁与弱点，计算出可能造成的影响。根据风险评估的结果，再针对无法接受的风险拟定对策，并考虑选择的对策所需的成本以及可能带来的效益，让风险值成为公司可以接受的程度，以便避免信息安全事件造成企业极大的损失。

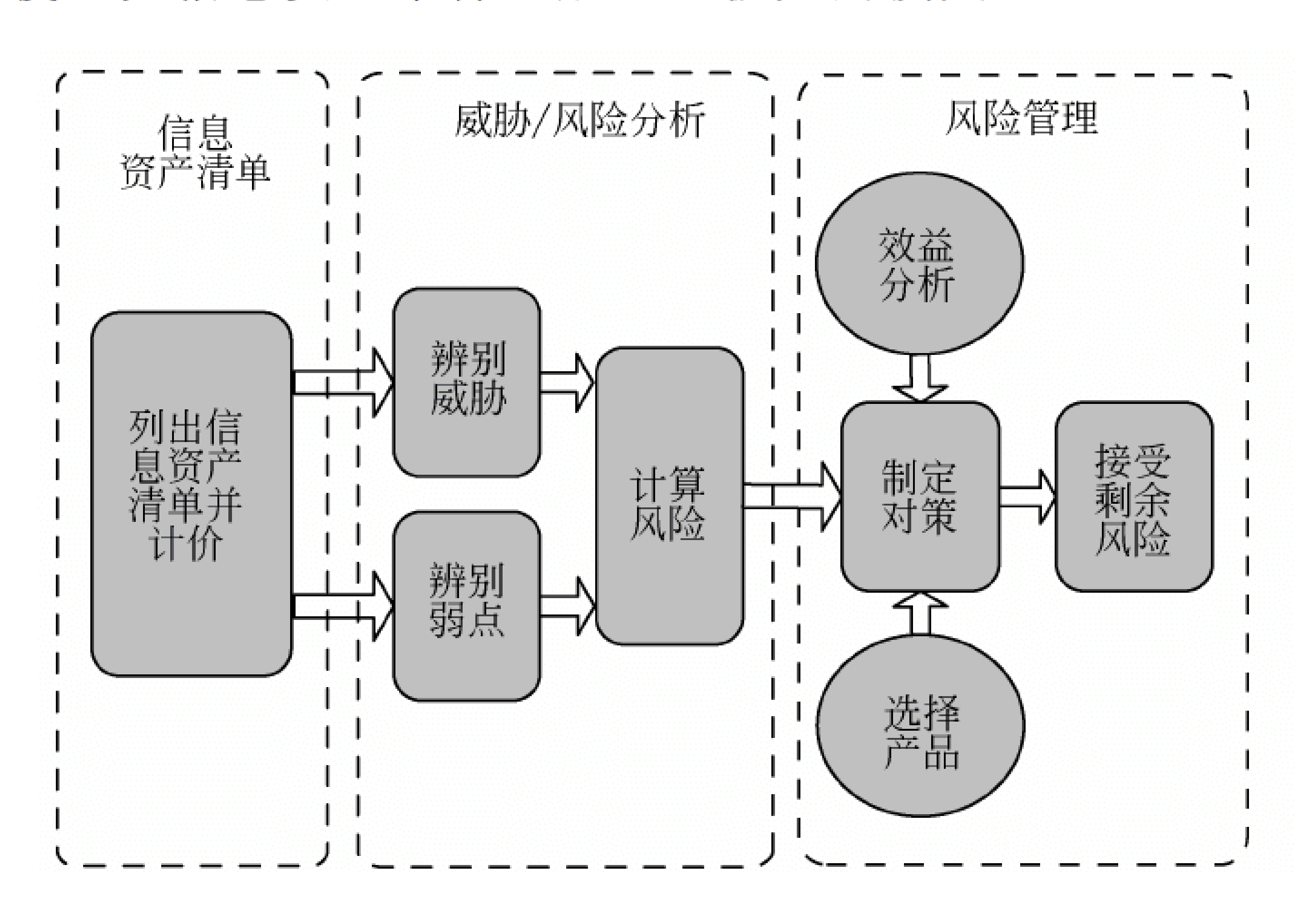


图 10-3　风险管理策略

风险值过高时，必须要采取对策。大致有以下两种对策：

（1）降低风险：导入信息安全措施或技术以消除或减少风险的威胁。例如，企业尚未安装防毒软件时，则极有可能遭受病毒的攻击。配置防毒软件并随时更新病毒码，即可将受病毒感染造成伤害的可能性降低。

（2）转移风险：除了降低风险之外，也可以将风险转移给其他单位承受。比如说通过保险的方式，将风险转嫁到第三者。如企业投保火险，一旦发生火警伤害，造成财产与业务上的损失，可以利用保险让保险公司实际承担大部分的财产损失伤害。

风险评估及管理的输出物为风险管理措施，这些将是后续改善措施制定的来源。

4）信息安全政策与组织

信息安全政策为一切信息安全执行事务的基础，且为组织执行信息安全事务的依循准则，故信息安全政策的发展不可不慎重。明确的信息安全政策方向，可以展现对信息安全的支持与承诺，而健全、有效率的信息安全组织才能使政策的制定、推广顺利进行。考虑信息安全事务的推广效率、企业高管的支持、涵盖范围的普及性、组织变更的弹性、资源的有效运用、决策及推动的联系等，根据实际状况设计如放射形态、联邦形态或中央形态等不同形态的信息安全组

织，才可以顺利推动信息安全管理体系。

5）安全管理流程

为符合信息安全政策的要求，以及利用管理措施降低风险，必须新增或修订现有的信息安全管理流程，以适当的信息安全管理措施，供员工作为落实信息安全的依据。

6）安全管理程序

信息安全流程中各项步骤的详细实施方式及责任必须明确，员工才会了解实际实施时要执行的工作内容。因此必须根据信息安全流程的内容，制定更为详细的管理程序。

7）信息安全培训

建立信息安全管理系统之后，内部许多原有措施可能已经修订，并增加了许多新的措施。因此必须策划实施员工的信息安全认知培训，让员工了解企业对信息安全的决心，以及相关的管制措施，并要求员工确实遵守，一起为公司的信息安全努力，以维持公司的竞争力。

8）安全需求定义

除了采取管理的方式来加强信息安全之外，适当的使用信息技术，也可以协助管理人员加强信息系统的安全性。因此，根据信息安全策略、政策的要求，以及相关管理流程或程序的需要，定义信息安全技术的需求，作为引进任何信息安全技术的评估标准，协助确保引进的信息安全技术可以满足公司的实际信息安全需求。

9）信息安全架构设计

信息系统的架构设计为信息安全的基础。良好的信息架构，可以支持各信息安全解决方案，通过信息技术提供企业可依赖的信息系统使用环境，按照不同的应用服务，会有不同的信息安全需求，而为了满足现有的信息安全需求，并提供引进未来信息安全技术的空间，必须要靠一套设计良好并可弹性扩充的信息系统架构才能提供各应用服务足够的安全性。一般而言，依据使用者访问的信任等级，将企业的 IT 基础设施（IT infrastructure）应分割成不同信息安全网域（security domain），不同信息安全网域彼此之间互相隔离，并经由边界服务（boundary service）保护（如 filter router、firewall 等），将数据按照重要性及服务对象分别置放于不同网域，并针对各网域建设不同的信息安全管控系统。这些信息安全管控系统，可以提供应用服务使用，以强化信息安全功能。

10）解决方案设计

根据风险评估的结果，部分风险管理的对策可能为信息安全技术或解决方案的导入。这步骤为根据选择的对策，参考企业的安全需求，以及现有的信息安全架构，设计该对策的解决方案。

11）产品选择

完成解决方案的设计之后，应该按照设计要点，考察业界目前已有的产品。根据产品的特性、优点及缺点，以及建设所需成本和建设之后可带给企业的效

益，选择可行的解决方案。

12）安全解决方案实施

选购信息安全产品之后必须开始建设。这时必须注意，除了确认产品中所需的关键功能均需建设之外，并应同时参考现行信息安全流程或程序，制定实际使用及管理的程序，并要求确切执行，以确保解决方案的实际效益。

13）安全控管与监测

所有的信息安全管理系统措施及信息安全解决方案，均应持续的监控，以了解目前状况，提早发现可疑事件，及掌握信息安全事件的发生。因此，信息安全管理的程序与流程必须包含控管与监测的部分，并必须按照规定实施。

14）安全管理评估

信息安全管理系统的实施成效，必须定期评估，才能了解是否确实有效，因此必须定期自行稽核。有效的稽核制度才能避免人员的倦怠、忽略，成为信息安全持续运作的主要推动力，提供信息安全的保证（assurance）。因此，除了在信息安全管理的程序与流程必须包含稽核制度的规定外，还必须制定实施计划定期主动稽核。

15）安全技术评估

由于信息系统与业务流程息息相关，因此包含信息系统架构、网络设备、服务器平台、应用系统等，均应定期评估目前使用技术的安全性，以及详细的实施状况，以了解其弱点及风险之所在，而加以管控。

2．信息安全框架导入的关键因素

按照上述的步骤，企业即可建设一套完整的信息安全管理体系，并搭配适当的信息安全技术，形成企业信息安全框架，提供一个安全使用信息的环境。但是实际的建设成效，仍有赖一些关键因素。企业要成功的导入信息安全框架，必须考虑以下几点：

1）取得高层授权

在实施任何信息安全方案之前，最重要的是取得充分的授权，而对于大型企业而言，这更是极为关键的重点。由于大型企业组织众多，一旦导入信息安全方案造成员工的工作习惯或流程必须变更，所带来的冲击也更为庞大。高级管理阶层的明确宣示，可以让员工明确感受到企业加强信息安全的决心。这些可以配合企业原有的文化，通过董事长或总经理所亲自签署寄发的电子邮件，以及在内部大型集会活动的正式宣达，都可以让员工了解企业对信息安全的重视，而主动去了解其自身所应做的改变。

2）选择合适的信息安全项目被访人

在进行现况评估时，大型企业常面临的问题为评估结果是否能确实代表企业目前的状况。现况评估的结果将会影响后续信息安全措施的选择与设计，因此遴选适当人选作为评估之受访对象，乃是成功的关键。受访对象应为相当熟悉该单位所有业务的主管，并对该部门的任务目标极为清楚。而受访人员在接受面谈之前，应先由其主管告知面谈的主要目的为了解现状，并非作为绩效考

评所用，因此应详细而清楚地说明现行状况，才可避免顾问人员忽略了现有的信息安全措施或缺点。

3）设计简单明了的信息安全政策

企业在建立信息安全政策的过程中，可以用以下几个简单的指标检查政策的适用性：

（1）兼顾安全防护及生产力；

（2）安全政策的执行度；

（3）简单扼要、易于理解。

此外，还需建立企业内部员工的安全认知，使每个员工都了解安全政策的目的，如此安全政策才能成功。

4）有效的安全认知培训

员工的安全认知乃是大企业在推行信息安全时最难执行，以及最不易了解成效的一部分。推动员工的安全认知，可以使员工了解信息安全的重要性，主动配合安全规定，养成良好的工作习惯，以下列出三个关键：

（1）传递信息：倡导员工安全常识之前，必须先决定倡导内容。过多繁复的内容将让员工不易吸收，然而过于片段的信息则会不易让员工了解实际的目的，因而员工不会确实执行。因此在倡导之前，必须先确认倡导的目标，并使用简明扼要不拗口的字句说明，最好可以让员工朗朗上口，效果更佳。

（2）传达机制：为了确保传达的有效性，必须要引起员工的兴趣与注意。常见的做法包含了透过寄给全公司的信件倡导，放在企业内部入口网站的首页，在重要的出入口张贴宣传海报等。此外，适当的举办一些活动，如举行有奖征答竞赛、鼓励员工参与信息安全口号设计等，均能有效地提高员工的注意力，进而增加他们对信息安全的认识程度。

（3）效果评估：透过效果评估，可以了解所有的认知训练活动成效。

5）确实稽核

良好的稽核可以协助确认信息安全措施的实际实施状况，也就是确保所有信息安全措施均有落实。例如，B 公司设立了独立的全球稽核单位，全年度在世界 170 个分公司进行信息安全的稽核，一旦被评为「不满意」等级，该分公司不仅须提出改善报告，相关人员并将遭到惩罚。另外，每位员工每年都需要完成信息安全自我稽核评估，切实地稽核平时对于信息安全的落实程度。除了可以确保信息安全措施的落实之外，更同时再次向员工宣示了公司对信息安全的重视程度与决心，使员工本身更加会注意个人在信息安全方面的责任。

6）善用顾问经验

许多大型企业在建设信息安全管理系统时，会邀请顾问公司的协助。由于顾问均为信息安全专家，且为独立的第三者，意见较为超然。因此应善用顾问的专业知识、经验及超然地位，利用顾问的力量以引导各单位形成实施信息安全的共识，并形成一股实施的力量，以加速信息安全措施与方案的导入及推行。

建设良好的信息安全环境是一件艰难的任务。清楚地掌握现有问题与弱点，缜密地评估各种风险，遵循既定的流程与规范不断改进以减轻信息安全事件可能带来的伤害，并持续要求落实各项信息安全措施，才能有效达到信息安全的目标，以最佳的状况持续支持企业的营运。

10.2 企业信息安全架构

10.2.1 安全架构定义

企业安全架构着眼于在整个企业组织架构中贯彻信息安全架构，而非针对单独的特定应用系统的具体功能性组件和运维结点，致力于建设一套能平衡企业组织架构中复杂业务流程、应用和系统的相关风险的战略性架构设计。

企业安全架构设计具有战略意义，它将比设计规范、拓扑图或拓扑配置拥有更长的生命周期，可发展成特定的方案。如果太过具体，它就会受限于当前的环境；如果太过广泛，它就不能起到提供指引的作用。应谨慎以防止架构变成某个具体实施的蓝图。

企业安全架构有以下作用：

（1）企业安全架构通过提供安全功能要求和实施方法来确保企业内实施一致的安全解决方案。

（2）根据业务需求事先定义所需的安全技术和解决方案。

（3）确保安全解决方案的相互可集成性以及相关的安全管控措施的到位和配合。

（4）确保安全组件的可重复利用，保护投资。

10.2.2 安全架构的通用性特征

企业安全架构具备以下特点：

（1）企业安全架构是一个长远的控制方案，而不是一个战术方案。

目前，企业的信息安全建设面临着大量的供应商所提供的各种各样的技术，可以实现各种复杂的安全控制措施，而各种异构的解决方案的重复建设和低效率将成为安全架构需着手解决的问题。安全架构总的趋势是为特定的执行情况而部署这些机制作为战术上的解决方案。而为了提供一个统一的观点和基于成本的考虑，优秀的企业安全架构设计是具有战略意义的。这意味着企业安全架构比规划蓝图、设计规范、拓扑图和配置等具有更长的生命周期。如果是过于具体，反而将制约当前的情况；如果是过于空泛或一般，则无法提供决策和指导。

在企业整体技术环境下，企业安全架构将为相关鉴别、选择、采集、设计、实施、部署和运维提供决策依据。

（2）企业安全架构的目标是共同的。

一个企业的安全架构应该支持多组织、多部门和多业务单元，描述安全控制及措施的长期技术趋势。它允许多种具体实现方式，取决于企业的安全现状和所处的阶段，应小心避免安全体系成为特定实施的蓝图。企业安全架构应该为整个组织机构提供一个全面风险管理的指导。

（3）企业安全架构提供了一个统一的共享安全控制的远景。

通过提供共享服务的模型，企业的安全架构着眼于从整体的角度来检查安全控制措施，识别出已有安全控制措施下的潜在风险，提供一个长远的改进计划。同时，这也是一个安全管理最佳实践的基本组成。

（4）企业安全架构提供了一个灵活的方式来处理当前和未来的威胁。

企业安全架构的所有基础组件的开发和部署只需要进行一次。在基础结构已经确定的前提下，其他架构组件就可以更容易被处理。如果基础架构引入新的举措，那么系统是不会引入新的弱点的。如果外部新的弱点被引入，则安全架构需要通过风险评估进行重新评估。

总而言之，企业安全架构（ESA）应该符合下述相关论述：

一个有效的安全规划应该承认和遵循：随着时间的推移，所有信息资产的价值和风险是变化的，而不是恒定不变的。

一个有效的安全方案运用最合适的技术来保护相关的资产，并结合执行和质量保障计划把风险减少到可接受的水平。

高质量的安全规划，包括经常性的管理审查和技术评估，以确保安全控制措施的有效并提供相关的反馈，使技术和方法适应资产的价值和风险，随着时间的变化而变化。图 10-4 给出了一个企业的安全架构。

安全治理、风险管理和合规
· 企业安全战略规划服务
· 安全管理差距分析服务
· PCI DSS合规遵从服务
· ISO 27001 认证指导咨询服务
· 信息安全管理体系咨询及设计服务
· 信息安全等级保护合规遵从服务
· 信息安全管理体系培训服务
· 企业信息系统风险评估服务

安全运维
· 安全运维管理中心设计及建设服务
· 安全事件响应流程设计服务
· 安全事件审计咨询服务
· 安全运维管理平台规划及建设服务
· 安全应急响应服务
· 安全事件审计平台的规划及建设服务
· 安全策略的开发及制定服务
· 安全绩效考核体系设计
· 操作行为审计平台规划及建设服务
· 管理安全服务

基础安全服务和架构

物理安全
· 机房物理安全评估服务
· 机房物理安全设计服务
· 智能视频监控平台建设服务

基础架构安全
· 基础架构安全评估服务
· 网络入侵防护系统
· 统一威胁管理系统
· 脆弱性管理系统
· 网络安全加固服务
· 主机入侵防护系统
· 主机访问控制系统
· 主机系统加固服务
· 终端安全控制系统

应用安全
· 应用开发生命周期安全评估和设计服务
· 应用系统代码审计服务
· 渗透测试服务
· 应用安全规范设计服务
· 应用安全评测服务
·Web 应用安全防护服务
· 网页防篡改服务
·Web 应用渗透测试及评估
· 应用开发环境安全评估及建设服务

数据安全
· 数据生命周期安全评估服务
· 数据安全管理规范设计服务
· 数据安全保护系统集成服务
· 数据敏感性分析服务
· 数据防丢失集成服务
· 数据加密保护服务
· 数据归档设计及实施服务
· 信息系统灾难恢复的规划及实施

身份 / 访问安全
· 统一身份及访问管理架构设计服务
· 统一身份及访问管理平台建设服务
· 强身份认证集成服务
· 应用系统身份及访问管理平台整合服务
· 企业单点登录（ESSO）集成服务
· 统一身份及访问管理帐号清理服务
· 统一身份及访问管理帐号管理流程设计及实施服务

图 10-4　企业安全架构

10.3　信息安全管理体系建设

信息安全管理体系（ISMS）是基于业务风险方法，建立、实施、运行、监视、评审、保持和改进信息安全的管理体系，即一套过程集框架，如图 10-5 所示。

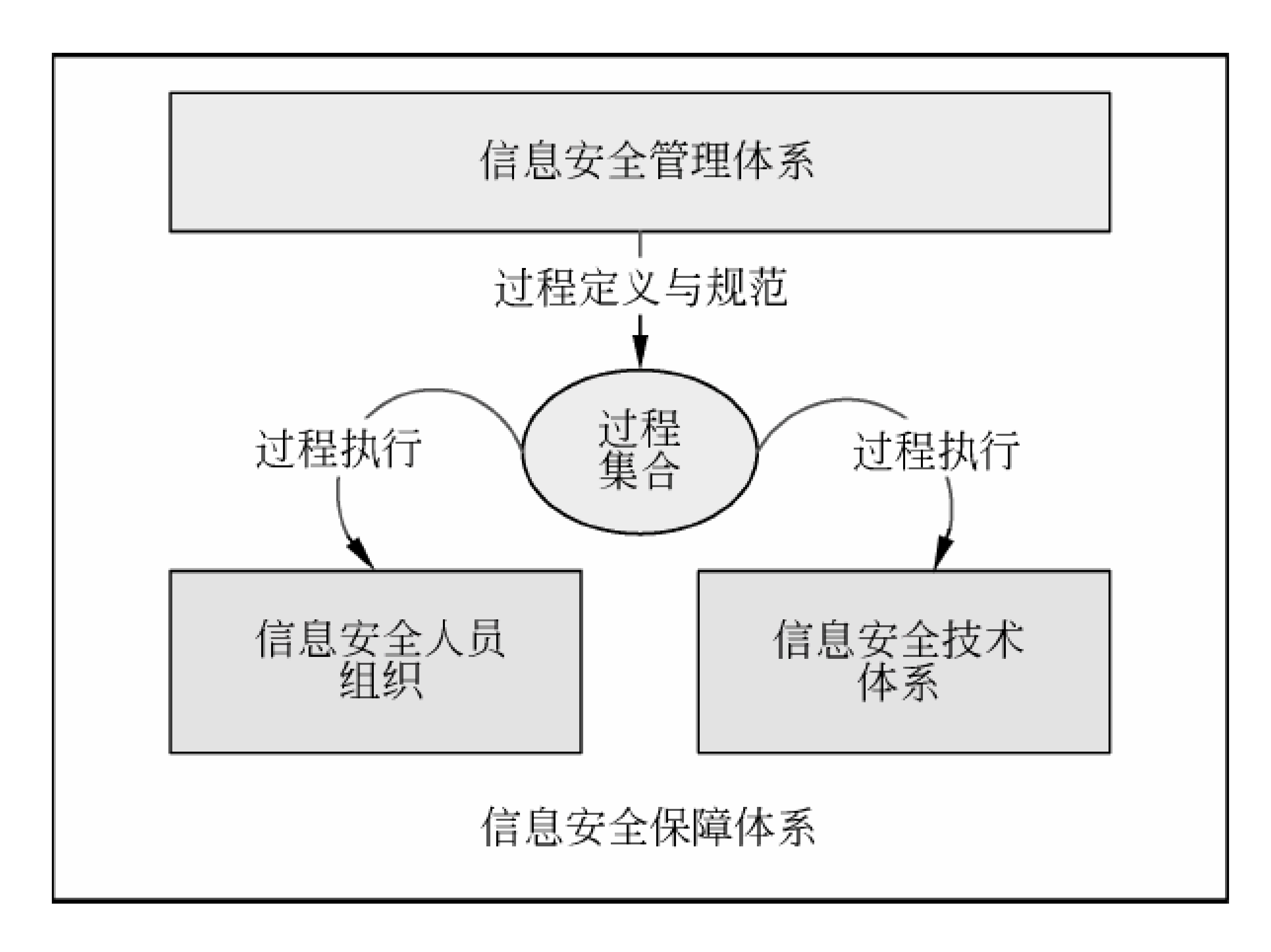


图 10-5 信息安全管理过程集框架

10.3.1 信息安全管理体系设计目标

建立健全信息安全管理体系对企业的安全管理工作和企业的发展意义重大，如图 10-6 所示。

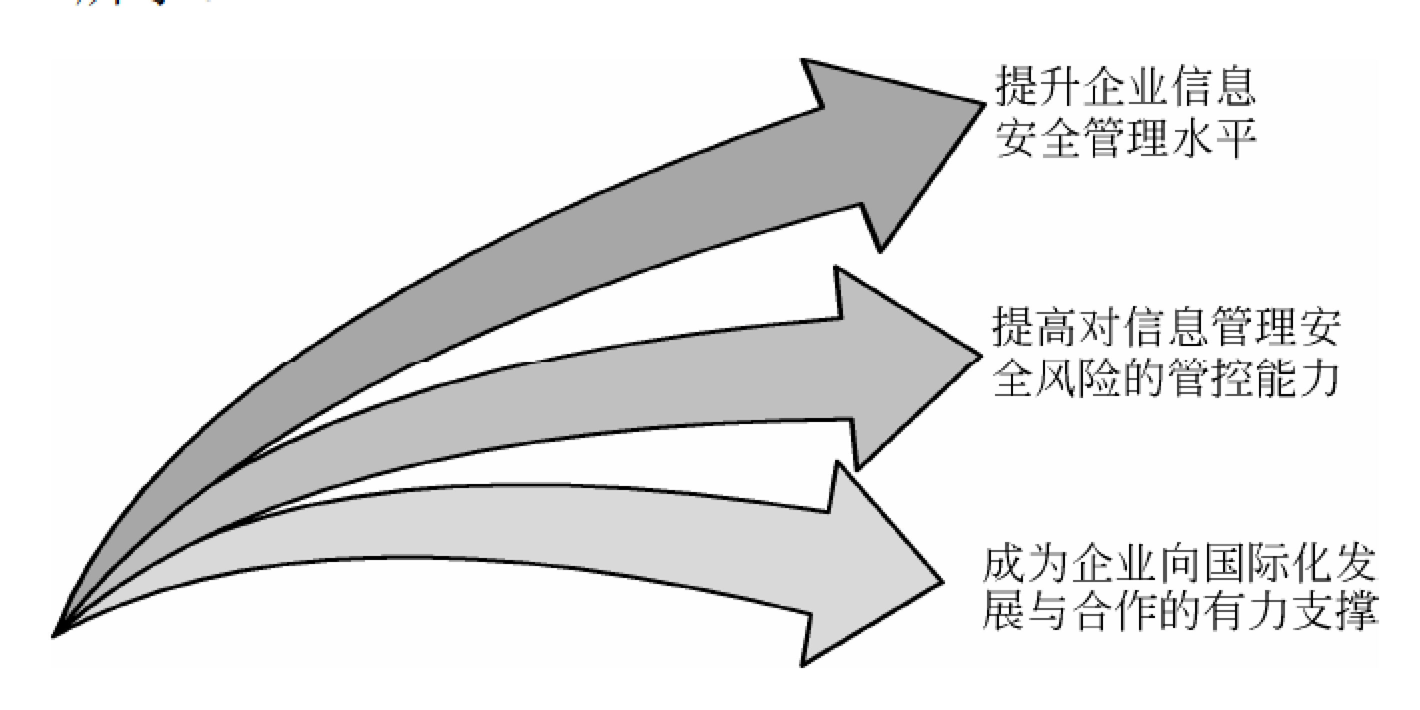


图 10-6 管理体系设计目标

首先，信息安全管理体系的建立将提高员工信息管理安全意识，提升企业信息安全管理的水平，增强组织抵御灾难性事件的能力，是企业信息化建设中的重要环节，必将大大提高信息管理工作的安全性和可靠性，使其更好地服务于企业的业务发展。其次，通过信息安全管理体系的建设，可有效提高对信息管理安全风险的管控能力，通过与等级保护、风险评估等工作接续起来，使得信息安全管理更加科学有效。最后，信息安全管理体系的建立将使得企业的管理水平与国际先进水平接轨，从而成长为企业向国际化发展与合作的有力支撑。

10.3.2 信息安全管理体系的建设

信息安全管理体系是组织在整体或特定范围内建立信息安全管理方针和目

标，以及完成这些目标所用方法的体系。它是基于业务风险方法，来建立、实施、运行、监视、评审、保持和改进组织的信息管理安全系统，其目的是保障组织的信息管理安全。它是直接管理活动的结果，表示成方针、原则、目标、方法、过程、核查表（checklists）等要素的集合，是涉及人、程序和信息技术的系统。

参照信息安全管理模型，按照先进的信息安全管理标准建立的全面规划、明确目的、正确部署、组织完整的信息安全管理体系，达到动态的、系统的、全员参与的、制度化的、以预防为主的信息安全管理方式，实现用最低的成本，保障信息管理安全合理水平，从而保证业务的有效性与连续性。组织建立、实施与保持信息安全管理体系产生的作用主要有下几点：

（1）强化员工的信息管理安全意识，规范组织信息管理安全行为；

（2）对组织的关键信息资产进行全面系统的保护，维持竞争优势；

（3）在信息系统受到侵袭时，确保业务持续开展并将损失降到最低程度；

（4）使组织的生意伙伴和客户对组织充满信心；

（5）如果通过体系认证，表明体系符合标准，证明组织有能力保障重要信息，提高组织的知名度与信任度；

（6）促使管理层坚持贯彻信息管理安全保障体系。

信息安全管理体系是一个系统化、程序化和文件化的管理体系，属于风险管理的范畴，体系的建立需要基于系统、全面、科学的安全风险评估。信息安全管理体现预防控制为主的思想，强调遵守国家有关信息管理安全的法律法规，强调全过程和动态控制，本着控制费用与风险平衡的原则，合理选择安全控制方式保护组织所拥有的关键信息资产，确保信息的保密性、完整性和可用性，从而保持组织的竞争优势和业务运作的持续性。

构建信息安全管理体系不是一蹴而就的，也不是每个企业都使用一个统一的模板，不同的组织在建立与完善信息安全管理体系时，可根据自己的特点和具体情况，采取不同的步骤和方法。但总体来说，建立信息安全管理体系一般要经过以下几个主要步骤，如图 10-7 所示。

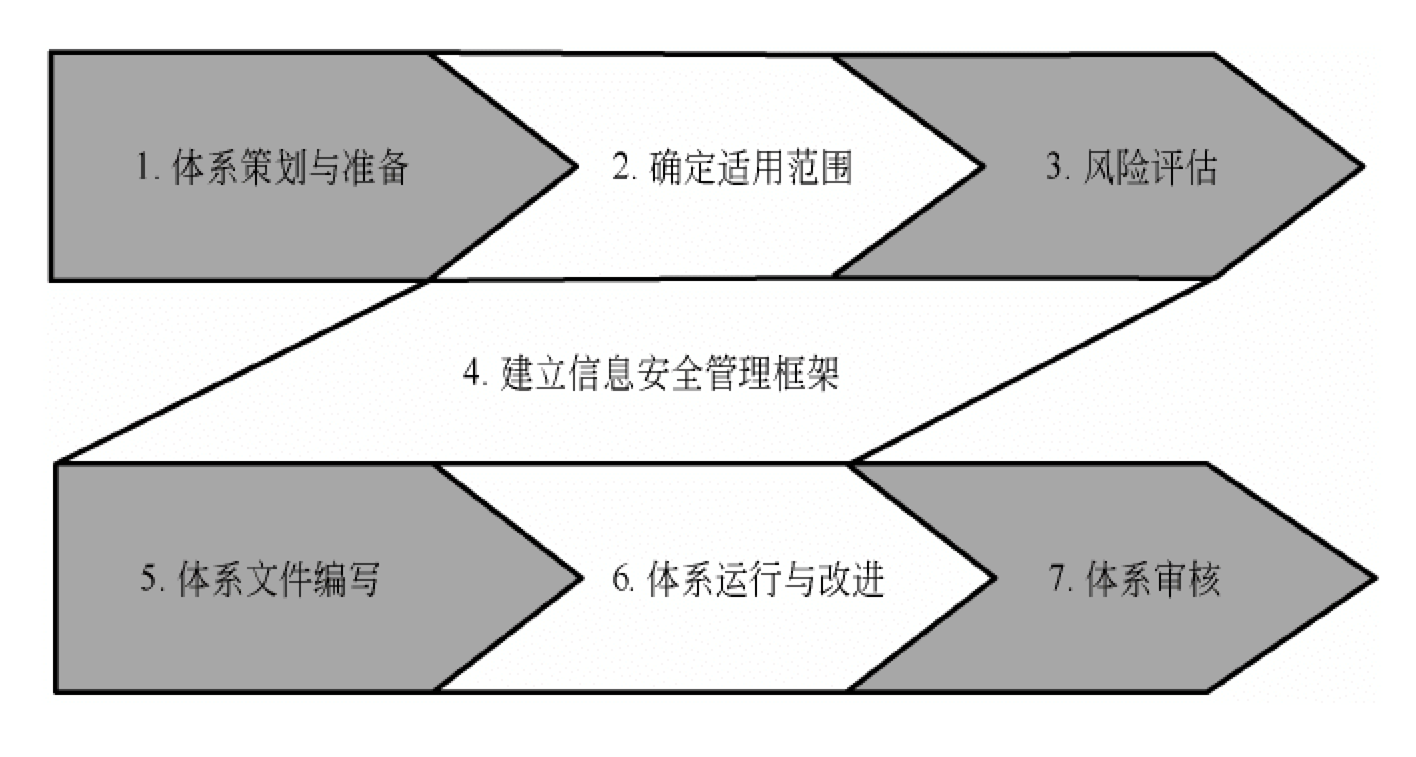


图 10-7　管理体系建设步骤

1. 信息安全管理体系策划与准备

策划与准备阶段主要是做好建立信息安全管理体系的各种前期工作，内容包括教育培训、拟定计划、安全管理发展情况调研，以及人力资源的配置与管理。

2. 确定信息安全管理体系适用的范围

信息安全管理体系的范围就是需要重点进行管理的安全领域。组织需要根据自己的实际情况，可以在整个组织范围内，也可以在个别部门或领域内实施。在本阶段的工作，应将组织划分成不同的信息管理安全控制领域，这样做易于组织对有不同需求的领域进行适当的信息安全管理。在定义适用范围时，应重点考虑组织的适用环境、适用人员、现有 IT 技术、现有信息资产等。

3. 现状调查与风险评估

依据有关信息管理安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的机密性、完整性和可用性等安全属性进行调研和评价，以及评估信息资产面临的威胁和导致安全事件发生的可能性，并结合安全事件所涉及的信息资产价值来判断安全事件一旦发生对组织造成的影响。

4. 建立信息安全管理框架

建立信息安全管理体系要规划和建立一个合理的信息安全管理框架，要从整体和全局的视角，从信息系统的所有层面进行整体安全建设，从信息系统本身出发，根据业务性质、组织特征、信息资产状况和技术条件，建立信息资产清单，进行风险分析、需求分析和选择安全控制，准备适用性声明等步骤，从而建立安全体系并提出安全解决方案。

5. 信息安全管理体系文件编写

建立并保持一个文件化的信息安全管理体系是 ISO/IEC 27001：2005 标准的总体要求，编写信息安全管理体系文件是建立信息安全管理体系的基础工作，也是一个组织实现风险控制、评价和改进信息安全管理体系，实现持续改进不可少的依据。在信息安全管理体系建立的文件中应该包含安全方针文档、适用范围文档、风险评估文档、实施与控制文档、适用性声明文档。

6. 信息安全管理体系的运行与改进

信息安全管理体系文件编制完成以后，组织应按照文件的控制要求进行审核与批准并发布实施，至此，信息安全管理体系将进入运行阶段。在此期间，组织应加强运作力度，充分发挥体系本身的各项功能，及时发现体系策划中存在的问题，找出问题根源，采取纠正措施，并按照更改控制程序要求对体系予以更改，以达到进一步完善信息安全管理体系的目的。

7. 信息安全管理体系审核

体系审核是为获得审核证据，对体系进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的检查过程。体系审核包括内部审核和外部审核（第三方审核）。内部审核一般以组织名义进行，可作为组织自我合格检查的基础；外部审核由外部独立的组织进行，可以提供符合要求的认证或注册。

信息安全管理体系的建立是一个目标叠加的过程，是在不断发展变化的技术环境中进行的，是一个动态的、闭环的风险管理过程，要想获得有效的成果，需要从评估、防护、监管、响应到恢复，这些都需要从上到下的参与和重视，否则只能是流于形式与过程，起不到真正有效的安全控制的目的和作用。

10.4　信息安全运维体系建设

企业安全运维包括威胁分析与预警、安全状态和事件的监控、安全事件或事故的响应，以及基于安全管控目标的操作行为和日志审计系统。这些安全运维的任务主要可通过安全事件监控、响应、审计以及相应的安全策略体系共同完成。安全运维体系包含服务于企业信息安全管理战略的管控目标和策略及相关的技术支持手段。企业信息安全运维体系的建设通常体现为安全运维中心的建设。

运维服务的发展趋势对应于企业的安全运维服务管理的发展，通常可以将其分为五个阶段：混乱、被动、主动、服务和价值阶段。混乱阶段：没有建立综合网管中心，没有用户通知机制；被动阶段：开始关注事件的发生和解决，关注信息资产，拥有了统一的运维控制台和故障记录及备份机制；主动阶段：建立了安全运行的定义，并将系统性能、问题管理、可用性管理、自动化与工作调度作为重点；服务阶段：已经可以支持任务计划和服务级别管理；价值阶段：实现性能、安全和核心应用的紧密结合，体现价值之所在。

目前，大多数企业的信息安全运维体系的服务水平处在一个被动的阶段。这主要表现在信息技术和设备的应用越来越多，但运维人员在信息系统出现安全事件的时候却茫然不知所措。究其原因，是该组织未建设成完整的信息安全运维体系。通常安全运维包含以下两层含义：

（1）在运维过程中对网络或系统发生病毒或黑客攻击等安全事件进行定位、防护、排除等运维动作，保障系统不受内、外界侵害。

（2）对运维过程中发生的基础环境、网络、安全、主机、中间件、数据库乃至核心应用系统发生的影响其正常运行的事件（包含关联事件）通称为安全事件；而围绕安全事件、运维人员和信息资产，依据具体流程而展开监控、告警、响应、评估等运行维护活动，称为安全运维服务。

10.4.1 信息安全运维体系设计目标

企业信息安全需要建立一个合理、高效的运维体系以适应信息化建设需要，成为亟待解决的问题。企业信息安全运维体系建设是将人、制度、流程以及技术平台贯穿融合，实行“一站式服务”，全过程跟踪，面向企业用户提供“端到端的服务”的基本机制。

10.4.2 信息安全运维体系的建设

首先，企业信息安全运维建立相关制度管理体系。

随着企业信息化建设从最初的系统开发，逐步转变为更多系统维护，工作格局改变。针对系统运行管理呈现的多元化、专业化的特点，运维制度必须做到原则性和可行性并举，核心原则是“重在落实”，让运维人员熟悉安全运维操作和故障处置流程，有利于防范因制度缺陷带来的风险；规范操作流程有利于避免误操作，减少人为失误和故障，缩短故障处理时间，确保各项系统运维操作都有据可依、有章可循；建立制度巡查体系，逐项落实各系统运维管理制度的执行情况，最大限度地查找安全隐患。

其次，安全运维人员管理体系建设。

信息安全运维中人员的 AB 角管理是核心。一是合理配置，运用资源。利用现有队伍力量，打破部门界线，进行交叉管理，确定重要业务系统运维管理员人选，实行 AB 角互备制度，明确相应管理权限和职责，发挥人力资源管理的整体功效，避免运维人员“单点故障”带来的风险。二是定期轮岗，优化互补。在系统运维中潜在的运行风险、安全威胁都与系统管理员授权行为有关，在确保系统运维工作连续性和稳定性的前提下，加强 AB 角定期轮岗，有效防范风险，促进运维人员全面熟悉各项业务系统，形成整体合力。三是分工明确，权责明晰。建立严格的 AB 角岗位责任制，按照“谁主管，谁负责”的原则，以达到分级管理，职责明确，相互监督的目的，确保不因某岗位人员缺位或空岗延误该办、急办的运维工作，避免因责任不清、人员不到位而出现推诿扯皮现象。

最后，安全运维，技术手段是重点。

加大系统的创新力度持续推动运维工作由“应急型”向“预防型”转变，如图 10-8 所示。

一是建立备份系统管理模式。重要业务数据采取集中异地备份模式，新增专用数据备份服务器，实现各种业务数据的自动备份，管理方案定制了严格的系统数据存储备份及恢复策略，利用集中式管理工具的帮助，运维人员可对全网备份策略进行统一管理，备份服务器可以监控所有机器的备份作业，修改备份策略，即时浏览所有目录。

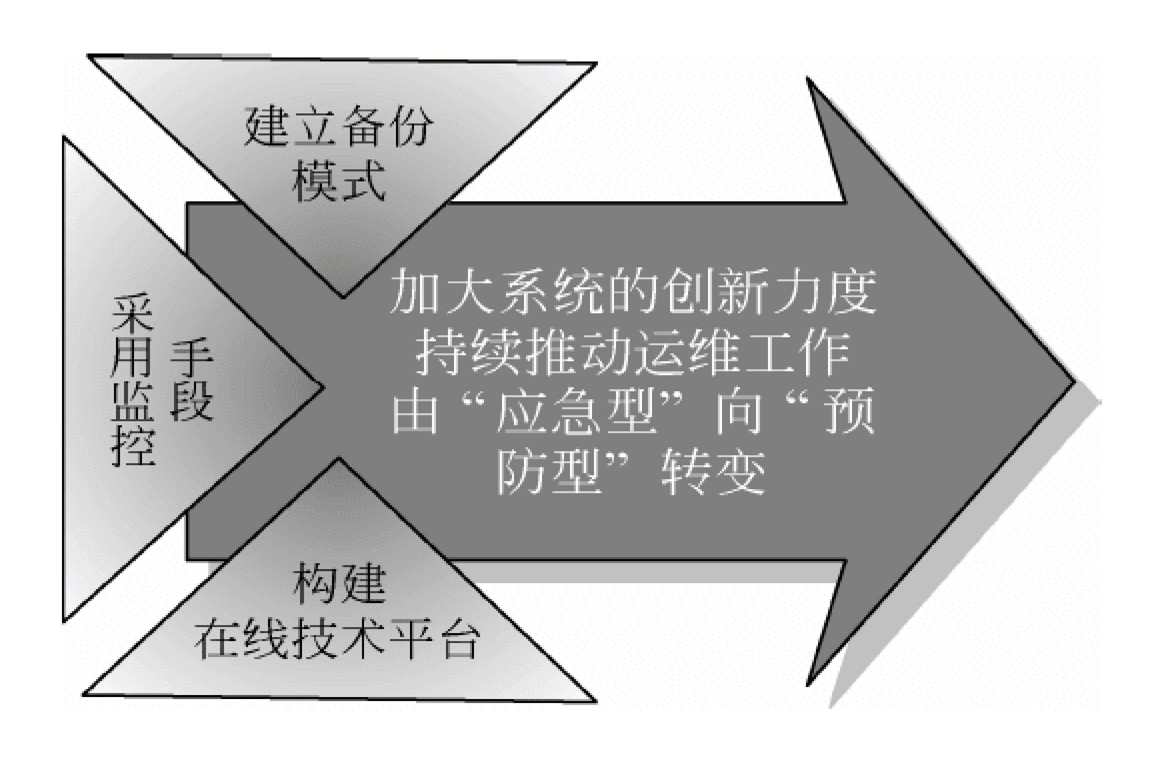


图 10-8　安全运维技术手段

二是采用先进监控技术手段。规划实施集中统一的安全运行管理中心，将分散在各信息安全监控基础设施管理系统中的各类事件数据、信息统一收集汇总并进行必要的格式转换，将事件数据集中到一个统一的事件数据库中，并实现统一监控管理。同时，也要建立初步的监控信息知识库和监控关联性分析引擎，增加运维技术管理监控层的有关功能，构建主动监控、预防故障发生。运维人员通过监控工具实现对不同服务对象和 IT 资源的实时监控，包括服务器、网络、业务应用和客户端等技术支撑管理子系统，通过集中监控管理平台对不同被管对象的技术支撑管理子系统进行综合处理和集中管理。当系统超过设定阈值自动报警时，通过系统间的关联分析，运维人员可主动发现并解决故障；通过趋势分析，寻找潜在故障，防患于未然，改变“被动救火”的局面。引进机房设备监控系统对配电系统、门禁系统以及消防系统等进行集中监视及控制，把各功能模块完全无缝集成在统一应用平台之中。使用专门的服务器或工作站监控重要业务系统机房环境，同时收集、记录、保存、管理各系统中的重要信息及数据，对于重点保护设备的运行及报警信号有手机短信自动接收功能。

三是构建在线技术服务平台。建立 FTP 服务器，实行集中管理，建立运维资源库，由运维人员将相应系统从建设之初至运行期间所收集的各类运维事件、常见问题及维护技巧，及时补充到资源库中，以备在运维工作中随时查找调用。实现系统故障自助处理，减少维护工作量，实现系统运维工作的智能化。

10.5　信息安全技术体系建设

充分利用信息安全的技术手段（包括身份认证、访问管理、内容安全、审核跟踪和响应恢复等），同时结合信息安全所保护的对象层次，以及目前主流的信息安全产品和信息安全技术，完善企业信息安全技术体系框架。企业信息安全技术体系层面如图 10-9 所示。

1．物理层安全

物理层安全主要包括物理位置的选择、物理访问控制、防盗窃和防破坏、

防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等。

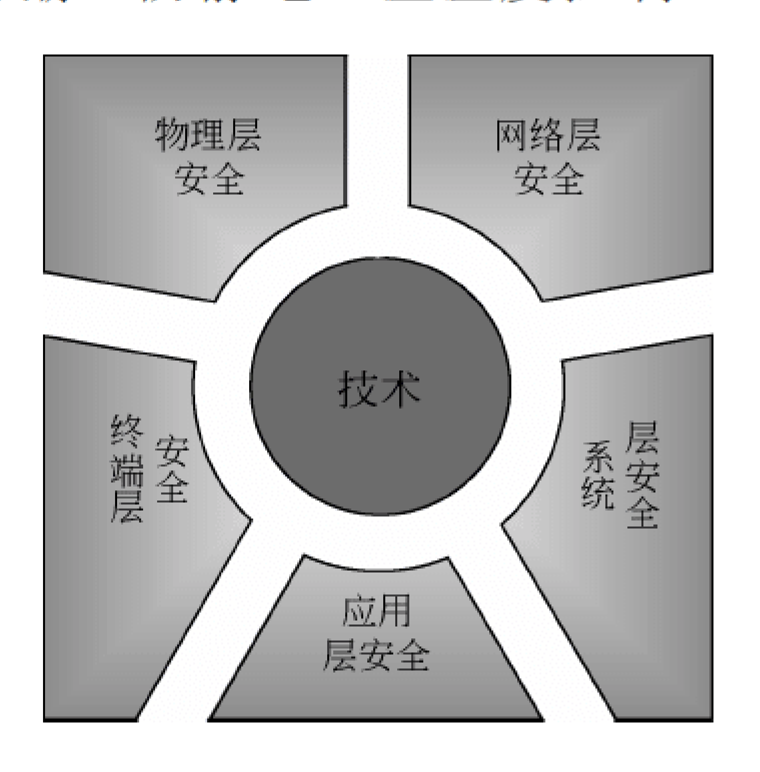


图 10-9 企业信息安全技术体系层面

2．网络层安全

网络层安全要注重安全域划分和安全架构的设计。可以根据信任程度、受威胁的级别、需要保护的级别和安全需求，将网络从总体上分成四个安全域，即公共区、半安全区、普通安全区和核心安全区。针对不同的安全区域采用不同的安全防范手段。

安全边界的防护：边界是不同网络安全区域之间的分界线，是不同网络安全区域间数据流动的必经之路。安全区域的边界防护是根据不同安全区域的安全需要，采取相应的安全技术防护手段，制定合理的安全访问控制策略，控制低安全区域的数据向高安全区域流动。针对 VPN（虚拟专用网）的接入安全控制，用户远程 VPN 接入主要用于员工出差时访问内部网络的需求和各企业小规模分支机构访问内部网络的需求。VPN 是为通过一个公用网络（通常是互联网）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。

网络准入控制：网络准入控制系统是通过对网络用户合法身份的验证以及对网络终端计算机安全状态的检测和评估，决定是否允许这台网络终端计算机接入企业网络中。若不符合制定的准入策略，将其放入隔离区以修复，或仅允许其有限地访问资源，降低非法用户随意接入企业网和不安全的计算机终端接入企业网对网络安全带来的潜在威胁。

做好网络设备登录认证：建立集中的网络设备登录认证系统，用于对网络设备维护用户的集中管理，认证用户的身份，决定其是否可以登录到网络设备；通过定义不同级别的用户，授权他们能执行的不同操作，记录并审计用户的登录和操作。

3．系统层安全

做好系统主机的入侵检测，针对系统主机的网络访问进行监测，及时发现

外来入侵和系统级用户的非法操作行为；做好系统主机的访问控制，系统主机访问控制提供给系统安全管理员最有效的方法，从用户登录安全、访问控制安全、系统日志安全等方面加入安全机制；做好系统主机的安全加固，定期对服务器操作系统和数据库系统进行安全配置和加固，在不影响业务处理能力的前提下对系统的配置进行安全优化，以提高系统自身的抗攻击性，消除安全漏洞，降低安全风险；做好主机的安全审计工作，提供全面的安全审计日志和数据，提升主机审计保护能力，对审计数据的访问进行严格控制，加强对审计数据的完整性保护。

4．应用层安全

随着各种各样的系统应用不断深化和普及，一些应用系统安全问题不断凸显出来。为了最大限度及时规避因应用安全问题带来的威胁，应着力抓好六个方面的工作：建立应用安全基础设施；健全应用安全相关规范；改进应用开发过程；组织关键应用安全性测试；加强应用安全相关人员管理；制定应用安全文档及应急预案。

5．终端层安全

加强终端计算机的安全管理。终端安全是指对接入企业网络的终端设备（主要是台式计算机、笔记本式计算机和其他移动设备等）进行的安全管理。其包括终端安全策略、防病毒、防入侵、防火墙、软硬件资产管理、终端补丁管理、终端配置管理、终端准入控制以及法规遵从等内容。

10.5.1 信息安全技术体系设计目标

一个合适的安全技术解决方案，不但需要理解安全管理的要求，用最小的投入得到最大的回报，同时也为安全运维管理提供了易于操作的平台。

在实施安全技术规划时，需要考虑以下内容：

（1）整体安全性的规划；

（2）对于不同的安全功能机制加以整合以达到统一控管及互补的目的；

（3）考虑对其他同时进行的项目的影响；

（4）从基础的、负面影响最小的安全措施入手；

（5）具有未来的扩充性，未来不致于因容量问题而需改变整体架构。

安全措施的设计与实施应当根据信息资产所面临的风险所定。安全措施的设计应以达到安全保护目的为原则而非最大幅度的投入。

企业信息化的进程中，由于企业网络的开放性、连通性和便利性，企业用户在享受各类共有信息资源的同时，也存在着信息可能被侵犯或被恶意破坏的危险。企业信息安全技术体系建设的目标就是保护有可能被侵犯或被破坏的信息不被外界非法操作者控制，业务系统不被恶意中断等，具体要达到机密性、

完整性、可用性、可控性等安全目标，如图 10-10 所示。

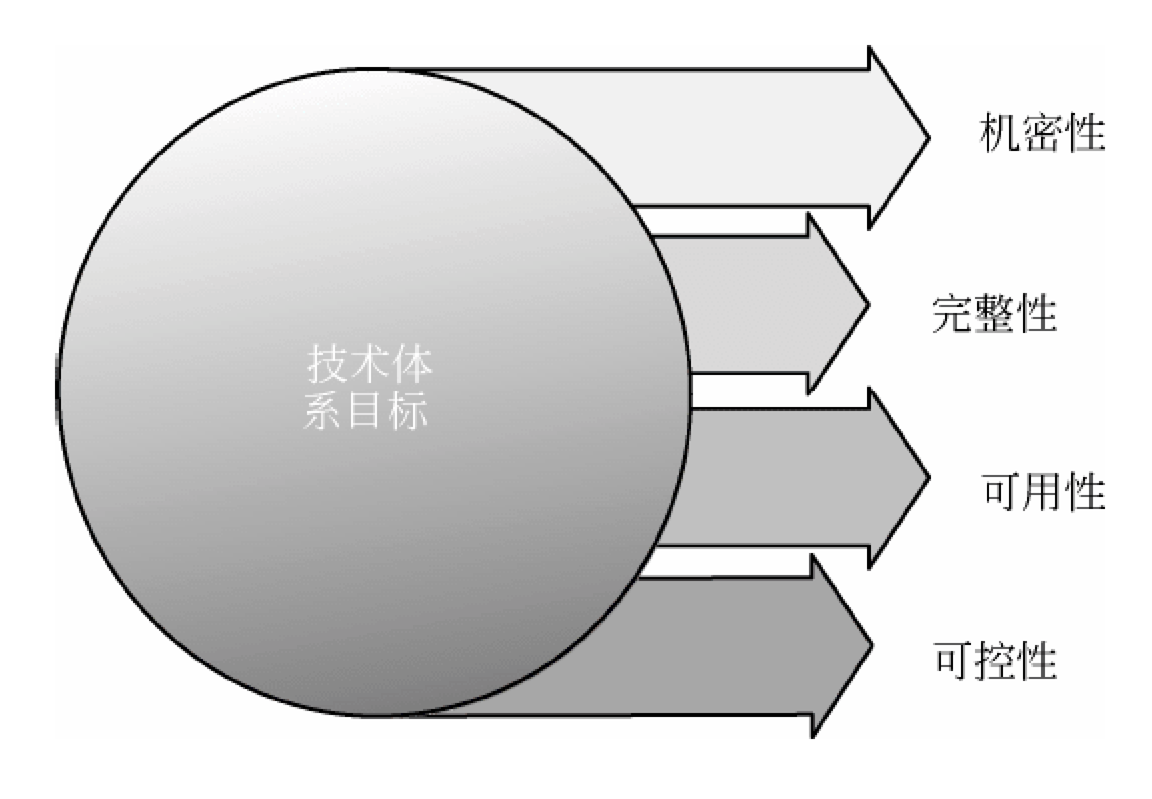


图 10-10　技术体系目标

企业信息安全技术防护体系应从终端源头、业务应用系统、服务器、网络等多方面，全面实现对用户违规操作的有效防范。通过以密码技术为支持、操作系统安全配置为核心，建立企业网内部的信任体系，对局域网内部的操作者进行身份认证和访问控制，对计算机终端和服务器进行重点保护，并实现安全与应用业务的有机结合，从而达到“主动”防御的目的。

10.5.2　信息安全技术体系的建设

企业信息安全技术体系建设要充分认识当前信息安全技术局限性，以主动防御为原则，以内网和信息安全为重点，在外部技术条件下，结合企业信息安全风险评估状况和业务发展要求，以企业信息安全框架为指导，建设统一规划、分布部署、集中管理的信息安全技术体系。信息安全技术建设主要包括以下内容：

1. 基于操作系统级的安全增强

建立可信计算机环境是安全建设的重要目标，作为可信计算机环境的核心，安全操作系统可提供全方位、高强度的安全性。

（1）强制与自主访问控制：内核级的高强度访问控制可使关键数据源和应用程序免受黑客和病毒攻击，可确保用户工作空间的独立性和可用性；

（2）确保操作系统提供服务的完整性；

（3）与密码技术的结合，实现更高强度安全：自动实现数据存储、传输和处理的高强度密码保障。

2. 应用的身份认证

身份认证是用户隔离的初级屏障，核心防护体系应采用基于密码技术的强认证，确保非授权用户不能对单机和所有应用服务器进行访问，并在此基础上，与基于特定应用程序的身份认证进行结合，变被动为主动防御。应用的身份认

证如图 10-11 所示。

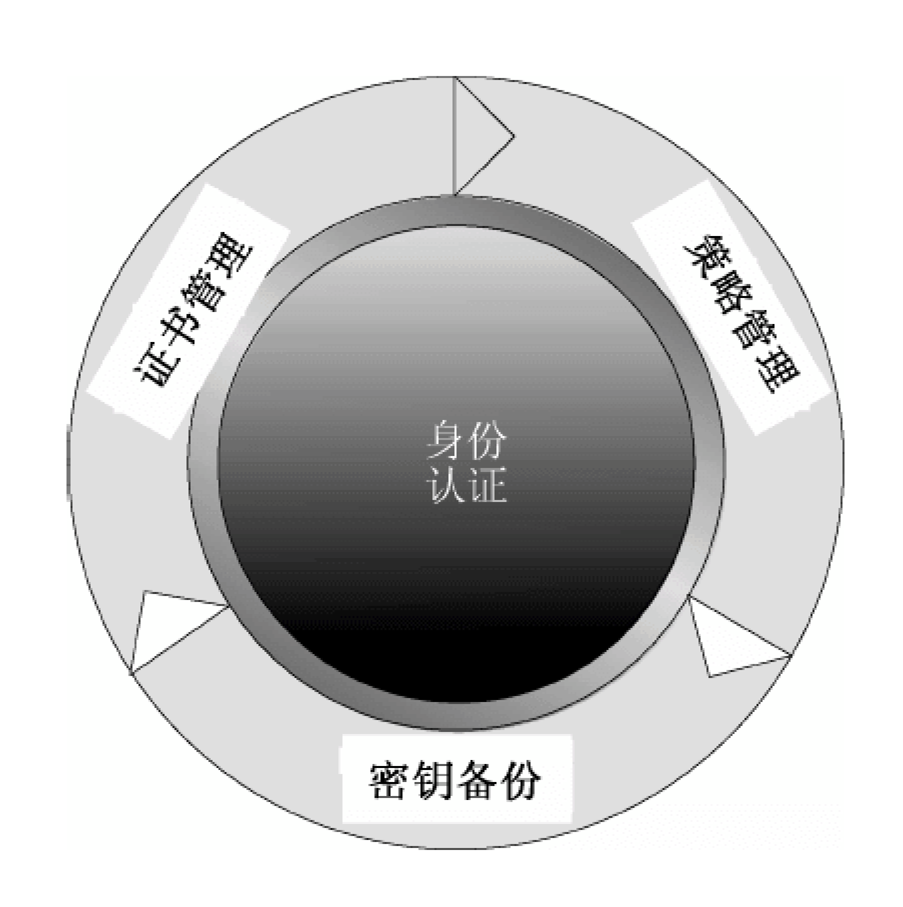


图 10-11　应用的身份认证

1）策略管理

在公钥基础设施（PKI）系统中，制定并实现科学的安全策略管理是非常重要的。这些安全策略必须适应不同的需求，并且能通过认证机构（CA）和注册机关（RA）技术融入到 CA 和 RA 的系统实现中。同时，这些策略应该符合密码学和系统安全的要求，科学地应用密码学与网络安全的理论，并且具有良好的扩展性和互用性。

2）密钥备份和恢复

为了保证数据的安全性，应定期更新密钥和恢复意外损坏的密钥是非常重要的，设计和实现健全自主、可控的密钥管理方案，保证安全的密钥备份、更新、恢复，也是关系到整个 PKI 系统强健性、安全性、可用性的重要因素。

3）证书管理与撤销系统

证书是用来证明证书持有者身份的电子介质，它是用来绑定证书持有者身份和其相应公钥的。通常，这种绑定在已颁发证书的整个生命周期里是有效的。但是，有时也会出现一个已颁发证书不再有效的情况，这就需要进行证书撤销，证书撤销的理由是各种各样的，可能包括工作变动到对密钥怀疑等一系列原因。证书撤销系统的实现是利用周期性的发布机制撤销证书，或采用在线查询机制随时查询被撤销的证书。

3. 加密机制

衡量一个加密技术的可靠性，主要取决于解密过程的难度，而这又取决于密钥的长度和算法。

1）对称密钥加密体制

对称密钥加密技术使用相同的密钥对数据进行加密和解密，发送者和接收者用相同的密钥。

2）非对称密钥加密体制

非对称密钥加密系统又称公钥和私钥系统，其特点是加密和解密使用不同

的密钥。非对称加密系统的关键是寻找对应的公钥和私钥，并运用密码技术使得加密过程成为一个不可逆过程，即用公钥加密的信息只能用与该公钥配对的私钥才能解密，反之亦然。

4．访问控制策略

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非法访问。它也是维护网络系统安全，保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用。下面分别介绍几种常见的访问控制策略，如图 10-12 所示。

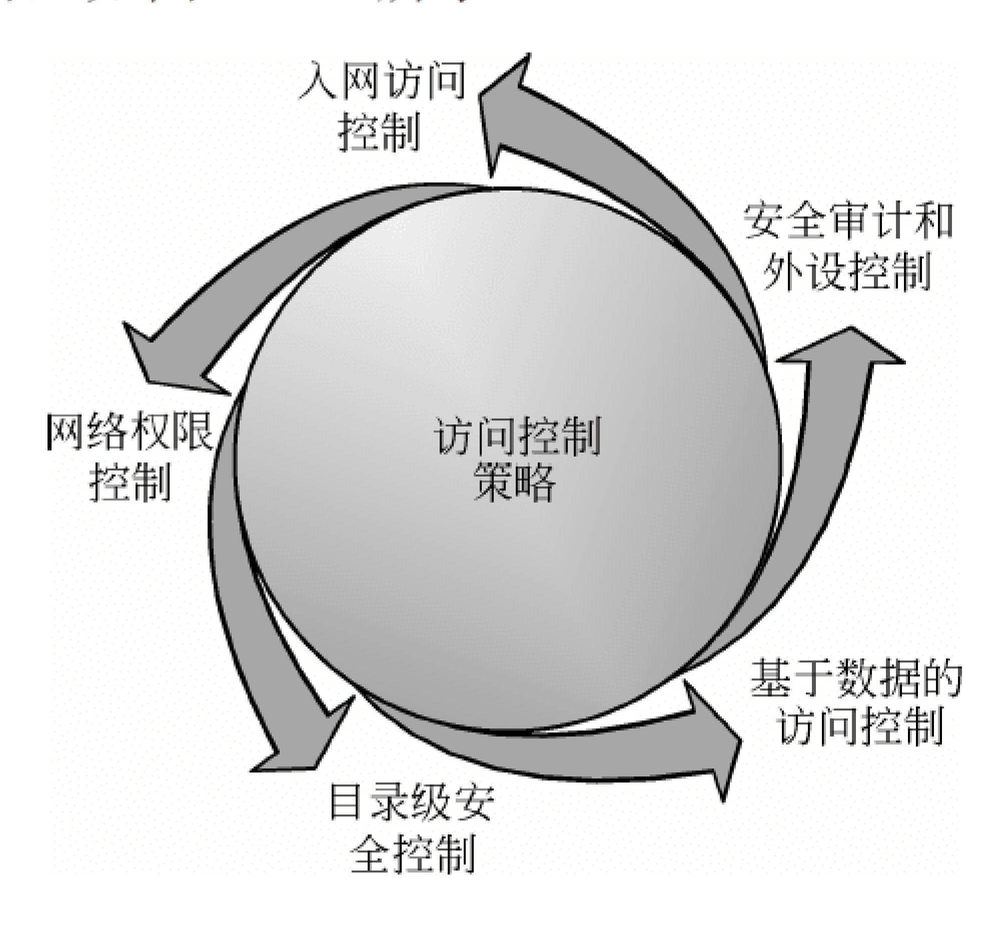


图 10-12 访问控制策略

1）入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，以及用户入网时间和入网地点。对用户名和口令进行验证是防止非法访问的首道防线。

2）网络的权限控制

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限，网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源，可以指定用户对这些文件、目录、设备能够执行哪些操作。我们可以根据访问权限将用户分为以下几类：

（1）特殊用户（即系统管理员）；

（2）一般用户，系统管理员根据他们的实际需要为他们分配操作权限；

（3）审计用户，负责网络的安全控制与资源使用情况的审计。

用户对网络资源的访问权限可以用一个访问控制表来描述。

3）目录级安全控制

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。这样可以让用户有效地完成工作，同时又能有效地控制用户对服务器

资源的访问，从而加强了网络和服务器的安全性。

5．基于数据的访问控制

在身份认证基础上的访问控制，应是基于最小数据单元、文件的细粒度访问控制，并与用户角色相关联，核心防护体系采用 RBAC（基于角色的访问控制技术）的授权访问控制技术实现与角色相关联的高强度访问控制。

6．安全审计和外设控制

安全审计系统主要是针对个人计算机及关键主机的操作行为进行审计，为事后的追踪提供依据，审计信息要尽量详尽，主要包括用户对应用程序、数据、文件和外设的各种操作。同时，对于外设的控制也是当前防止信息泄露的重要需求，核心防护体系设计的审计和外设控制重点针对个人计算机，同时也与成熟的主机审计与控制系统配合，实现整体的审计与控制。

7．防火墙技术

防火墙是一种网络安全保障手段，是网络通信时执行的一种访问控制尺度，其主要目标就是通过控制入、出一个网络的权限，并迫使所有的连接都经过这样的检查，防止一个需要保护的网络遭到外界因素的干扰和破坏。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监视了内部网络和 Internet 之间的任何活动，保证了内部网络的安全；在物理实现上，防火墙是位于网络特殊位置的一组硬件设备——路由器、计算机或其他特制的硬件设备。防火墙可以是独立的系统，也可以在一个进行网络互联的路由器上实现防火墙。用防火墙来实现网络安全必须考虑防火墙的网络拓扑结构。

8．VPN 技术

VPN 的安全保证主要是通过防火墙技术、路由器配以隧道技术、加密协议和安全密钥来实现的。利用 VPN 特性可以在 Internet 上组建世界范围内的 Intranet VPN。利用 Internet 的线路保证网络的互联性，利用隧道、加密等 VPN 特性可以保证信息在整个 Intranet VPN 上安全传输。利用 VPN 技术可以组建安全的 Extranet，既可以向客户、合作伙伴提供有效的信息服务，又可以保证自身的内部网络安全。

9．多层次多级别的防病毒系统

防病毒产品可以自动进行文件更新，使管理和服务作业合理化，并可用来从控制中心管理企业范围的反病毒安全机制，优化系统性能、解决及预防问题、保护企业免受病毒的攻击和危害，并对采用 HTTP、FTP、SMTP 协议进入内部网络的文件进行病毒扫描和恶意代码过滤，从而实现对整个网络的病毒防范。

10. 入侵检测

入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。

11. 操作系统内核加固体系

目前，一个新漏洞的发布往往伴随着新的病毒以及攻击手段的出现。而传统的防毒、漏洞扫描、入侵检测等基于知识库或者特征库识别的防范技术面对这种新生的甚至未知的攻击手段往往无能为力。信息安全的根本解决，需要通过建立安全操作系统，构建动态、完整的安全体系。对原有操作系统进行内核安全加固，是当前必须的增强重要服务器和计算机终端安全性的办法。操作系统内核加固基于主机和终端的系统内核级安全加固防护，通过采用强制访问控制、强认证（身份鉴别）和分权管理的安全策略，作用范围从系统内核层一直延伸到应用层，从而对操作系统内核实施保护，对网络中的不安全因素实现“有效控制”，构造出一个具有“安全内核”的操作系统。从根本上阻止针对操作系统关键资源的破坏，有效地遏制传统安全防护技术防已知难防未知造成的安全威胁。这样既可以有效覆盖其他安全技术产品的防护盲区，又可以弥补防护上的不足。

10.6 建立纵深的信息安全防御体系

信息安全保障应当建立纵深防御体系，什么是纵？什么是深？纵是从三个层面（事前、事中、事后）进行全面控制；深是从三个方向（管理体系、技术体系、运维体系）进行深入防御，如图 10-13 所示。

纵：正如信息安全这四个字所表现的一样，以保护信息为其最重要的目的。那么就应当对信息安全事件发生的之前、之中和之后进行有效控制。即以预防控制为主，但是也不能忽略操作性控制和恢复性控制。因此，应当从信息的事前预防、事中监控和事后恢复三个层面建设信息安全。

深：信息安全涉及的领域非常广，对人员、硬件、数据、软件等方面都会涉及。我们需要从管理体系、技术体系、运维体系三个方面的深度进行概括，并形成企业信息安全框架或空间。

管理体系：人是实施信息安全的最关键的因素，人控制好了，信息安全就控制好了。因此成立一个合理和有效的安全组织架构，对于保证安全日常运行是最重要的。建立一个成功的信息安全组织体系有很多关键环节，但是组织高层管理者的参与、安全纳入绩效考核、人员信息安全意识与技能培训是必不可

少的成功因素。

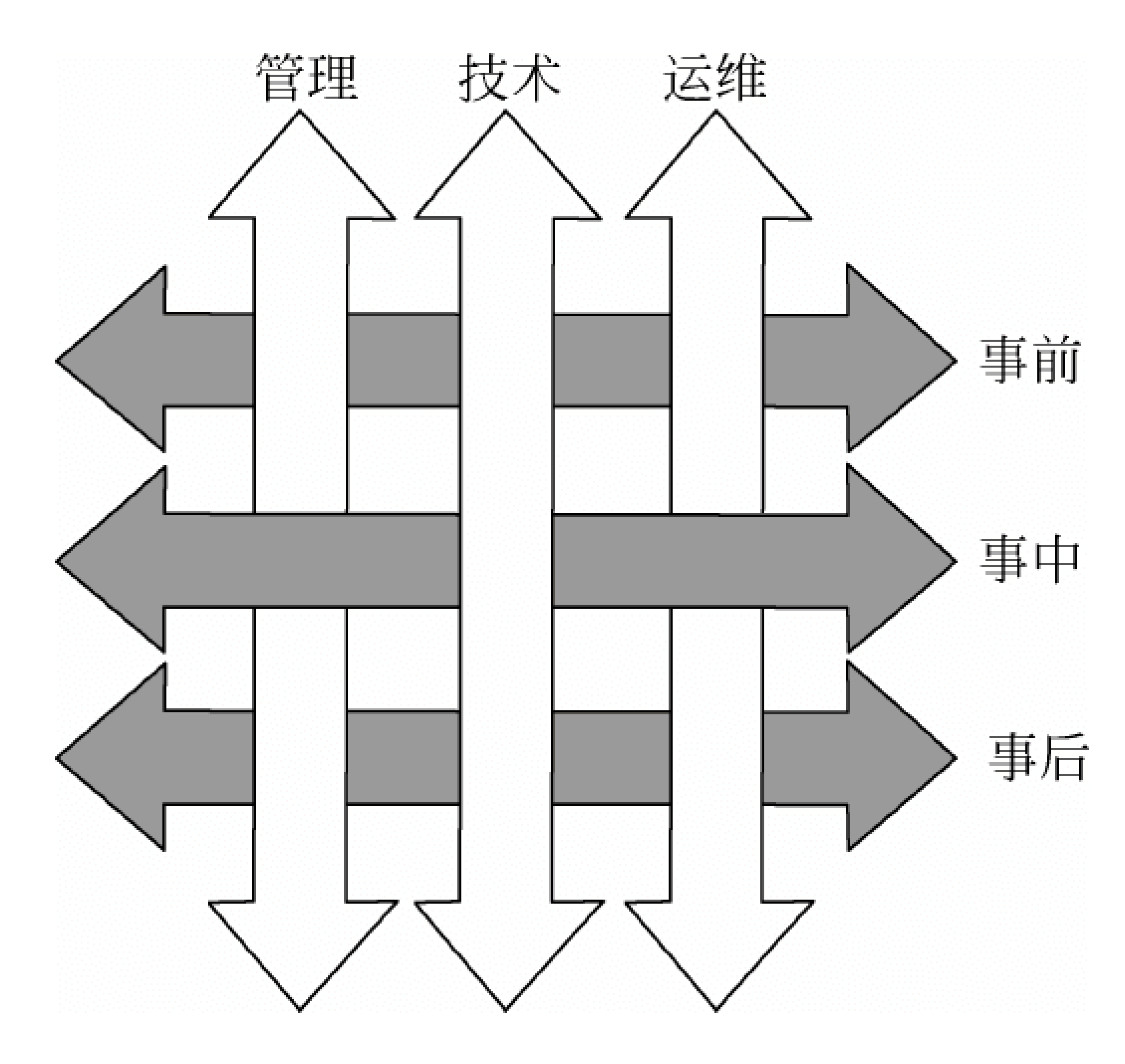


图 10-13　企业信息安全纵深防御体系

把信息安全好的做法固化下来形成规则，就是制度。因此，信息安全制度是组织中的信息安全行为准则。信息安全保障体系只有做到制度化、规范化才能更好地保证事前预防、事中监控和事后审计等安全措施的执行与落实。

技术体系：技术是安全必不可少的实施工具，采取哪些安全技术，市场上有哪些工具可以使用，这是绝大部分信息安全管理工作者最关心的话题。一般来说，可以按照从上到下信息所流经的设备来部署工具，即从数据安全、终端安全、应用安全、操作系统与数据库安全、网络安全、物理安全六个方面来选择不同的安全工具。信息安全工具种类繁多，一般来说，每一种工具都有其擅长的安全方面，因此应按照“适度防御”原则，综合采用各种安全工具进行组合，形成企业“适用的”安全技术防线。最后，需要一到两种提供综合管理的工具来帮助把所有的安全监控工具进行统一管控。这个和最终希望呈现给使用者的目的有所不同。例如，SOC（安全运行中心）是给企业日常维护管理者使用的，IYRM（风险管理工具）作为综合风险呈现，是给企业风险或安全管理层使用的。

运维体系：技术体系更多是解决安全风险点的问题，也就是我们常说的“就事论事”：有病毒杀病毒，有漏洞补漏洞等等。但是我们知道，信息分散在一系列工作流程的各环节中，因此需要对各项日常运行工作流程进行安全控制，也就是从信息的生命周期进行流程控制，即在信息的创建、使用、存储、传递、更改、销毁等各个阶段进行安全控制。目前受到热捧的开发安全就是在信息创建阶段的一个细化控制手段。在运行体系建设中，往往需要结合 ITIL、COBIT 等流程分析来关注信息的生命周期安全。自美国“9 • 11”事件以后，业务连续性的重要程度提到了前所未有的高度，包括灾备中心建设、业务连续性计划、应急响应等等都有相应的标准与理论支持，特别是 BS 25999 标准的颁布，给如何建立一套完善的应急体系提供了参考。

第11章 信息安全建设案例

在前面 10 章对信息安全的基本概念、发展历程、标准体系、建设框架以及建设的策略和方法论述的基础上，本章分别从信息安全体系方案、规划管理、运维体系实践以及技术体系建设等实际案例的描述给读者一个对信息安全建设全面的体验，以便让读者进一步理解和掌握信息安全建设的基本知识、策略和方法，形成一个企业信息安全建设的基本思路，打赢信息安全保卫战。

11.1　信息安全体系方案案例

本案例给出了一个典型的企业信息安全解决方案。其主要是基于前几章描述的基本信息安全框架概念和策略方法，在进一步结合一个典型的企业实际情况，形成一个企业实际信息安全体系的解决方案。

11.1.1　项目概述

1. 信息安全建设思路

一个典型企业的信息安全建设工作的总体思路如图 11-1 所示。

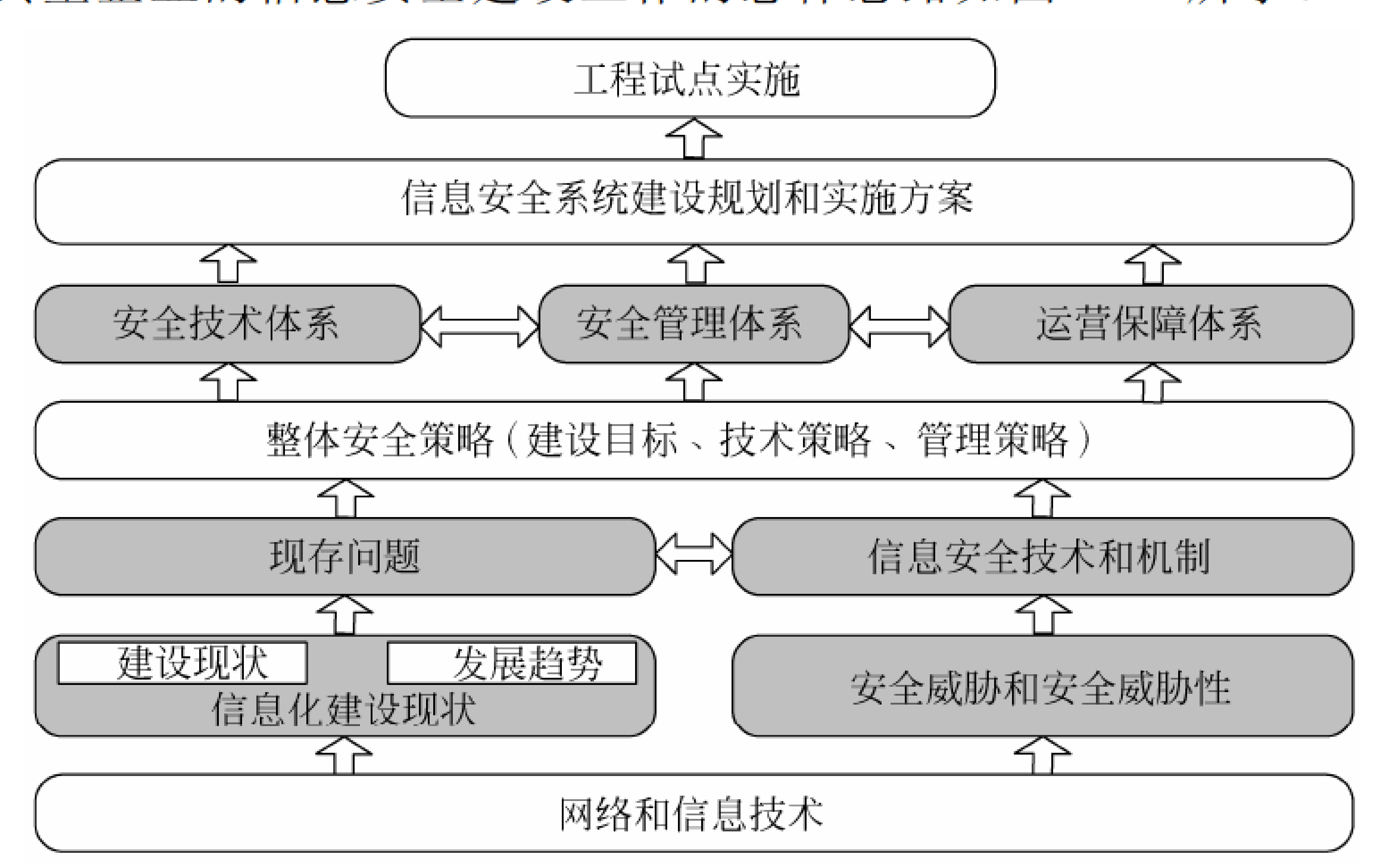


图 11-1　一个典型企业的信息安全建设思路

这个典型的企业信息安全建设由针对性安全问题和支撑性安全技术两条主线展开，这两条主线在安全建设过程中的关键点又相互衔接和融合，最终形成一个完整的安全建设方案，并实施落地。

首先，企业的信息化建设是基于当前通用的网络与信息系统基础技术的，这使得信息化建设和安全技术有了一个共同的基础，使得企业的针对性安全需求与通用的安全解决技术和方案有了一定的共同点和结合点。

在这个基础上，通过安全评估，对信息化建设和信息安全建设进行分析和总结，其中包括对建设现状和发展趋势的完整分析，归纳出系统中当前存在和今后可能存在的安全问题，明确网络和信息系统运营所面临的安全风险级别。

从支撑性安全技术的主线展开，从现有网络和信息技术的固有缺陷出发，总结了普遍存在的安全威胁，并根据其他系统中的信息安全建设实践中的经验，从信息安全领域的完整框架、思路、技术和理念出发，提供完整的安全建设思路和方法。

在此基础之上，两条主线进入融合的阶段。信息安全领域的理论、框架和技术基础与企业的安全问题有机地进行结合，有针对性地提出企业安全保障总体策略。在这个安全保障总体策略中，包括了整体建设目标、安全技术策略，以及相应的管理策略。总体安全策略一方面充分体现了企业对自身信息化建设中安全问题的针对性，另一方面也充分基于现有的信息安全领域的安全模型和技术支持能力，因此具备了可行性、针对性和前瞻性。

以安全保障总体策略为核心，分三个方面进行整体信息安全体系框架的制定，包括安全技术体系、安全管理体系和运营保障体系。在现实的运营过程中，安全保障不能够纯粹依靠安全技术来解决，更需要适当的安全管理，相互结合来提高整体安全性效果。

在信息安全体系框架的指导下，依据相应的建设标准和管理规范，规划和制定详细的信息安全系统实施方案和运营维护计划。

为了更加稳妥地进行全面的信息安全建设，在信息安全系统实施过程中首先进行试点项目建设，在试点项目建设中进一步积累经验，并对某些实施方案的细节进行调整，为建设实施顺利地全面开展打下基础。

信息安全体系建设的思路体现了以下的特点：

（1）统筹规划和设计在建设过程中占有非常重要的地位；

（2）充分结合建设现状与信息安全通用技术和理念；

（3）充分考虑了当前的建设现状以及未来业务发展的需要；

（4）注重安全框架概念的形成，以及管理、技术和保障的相互结合；

（5）采取试点工程计划，使得信息安全建设实施更加稳妥。

2. 信息安全建设内容

基于这个典型企业的实际情况，信息安全建设所涉及的工作内容主要包括以下部分：

1）建立管理组织机构

建立专职的信息安全监管机构，明确各级管理机构的人员岗位配置和职能权限，全面负责信息安全建设工作和维护信息安全系统的运营。

2）物理安全建设

按照国家对于计算机机房的相关建设标准，制定统一的计算机机房建设标准和管理规范，对于计算机机房建设中的环境参数、保障机制，以及运行过程中的人员访问控制、监控措施等进行统一约定，颁布统一的计算机机房管理制度，对设备安全管理、介质安全管理、人员安全管理等作出详细的规定。

3）网络安全建设

网络安全是信息安全保障的重点，制定统一的网络结构技术标准，对如何划分内部信息系统的安全区域及安全区域的边界采取的隔离措施进行约定，保证内部网络与外部网络、办公网与业务生产网之间的安全隔离。

制定统一的互联网接入点、外联网接入点的技术标准和管理规范，统一约定网络边界接入点的网络结构、安全产品的部署模式，保证内部网络与外部网络之间的安全隔离。

制定统一的远程移动办公技术标准和管理规范，保证远程移动办公接入的安全性。

制定统一的网络安全系统建设标准和管理规范，包括防火墙、网络入侵检测、网络脆弱性分析、网络层加密等。

4）系统安全建设

系统安全的工作内容包括制定统一的系统安全管理规范，包括主机入侵检测、系统安全漏洞分析和加固， 提升服务器主机系统的安全级别。

制定统一的网络病毒查杀系统的建设标准和管理规范，有效抑制计算机病毒在内部网络和信息系统中的传播和蔓延。

5）应用安全建设

应用安全机制在应用层为业务系统提供直接的安全保护，能够满足身份认证、用户授权与访问控制、数据安全传输等安全需求。

制定统一的身份认证、授权与访问控制、应用层通信加密等应用层安全系统的建设标准和管理规范，改善业务应用系统的整体安全性。

6）系统和数据备份管理

系统和数据备份是重要的安全保障机制，为了保障业务数据的安全性，降低突发意外事件所带来的安全风险，制定统一的系统和数据备份标准与规范，采取先进的数据备份技术，保证业务数据和系统软件的安全性。

7）应急响应管理

制定统一的应急响应计划标准，建立应急响应计划，包括安全事件的检测、报告、分析、追查和系统恢复等内容。在发生安全事件后，尽快作出适当的响应，将安全事件的负面影响降至最低，保障金融业务正常运转。

8）灾难恢复管理

灾难是指对网络和信息系统造成任何破坏作用的意外事件，要制定详细的

灾难恢复计划，考虑到数据大集中的安全需求，采用异地容灾备份等技术，确保数据的安全性和业务的持续性，在灾难发生后，尽快完成恢复。

9）人员管理和教育培训

制定统一的人员安全管理和教育培训规范，定期对信息系统的用户进行安全教育和培训，对普通用户进行基本的安全教育，对安全技术岗位的用户进行岗位技能培训，提高全员的安全意识，培养高素质的安全技术和管理队伍。

11.1.2　信息安全建设的基本方针

这个典型企业信息安全体系建设的基本安全方针是“统一规划建设、全面综合防御、技术管理并重、保障运营安全”。

统一规划建设，突出了进行统筹规划的重要性，提供了企业安全框架、安全建设所需的统一技术标准和管理规范，以及实施步骤的安排，也保证了人员和资金的投入。

全面综合防御，是指在技术层面上，综合使用了多种安全机制，将不同安全机制的保护效果有机地结合起来，构成完整的立体防护体系。

技术管理并重，突出了安全管理在信息安全体系中的重要性，仅仅凭借安全技术体系无法解决所有的安全问题，安全管理体系与技术防护体系相互配合，增强技术防护体系的效率和效果，同时也弥补当前技术无法完全解决的安全缺陷，实现了最佳的保护效果。

保障运营安全，突出了安全保障的重要性，利用多种安全保障机制，保障了网络和信息系统的运行安全，也保障了业务的持续性和业务数据的安全性。

11.1.3　信息安全建设的目标

根据企业信息安全体系建设的基本方针，企业信息安全建设的目标，可以用“一个目标、两种手段、三个体系”进行概括。

1．一个目标

企业信息安全建设的目标是：基于安全基础设施、以安全策略为指导，提供全面的安全服务内容，覆盖从物理、网络、系统直至数据和应用平台各个层面，以及保护、检测、响应、恢复等各个环节，构建全面、完整、高效的信息安全体系，从而提高企业信息系统的整体安全等级，为企业的业务发展提供坚实的信息安全保障。

2．两种手段

信息安全体系的建设应该包括安全技术与安全管理两种手段，其中安全技术手段是安全保障的基础，安全管理手段是安全技术手段真正发挥效益的关键，

管理措施的正确实施同时需要有技术手段来监管和验证，两者相辅相成，缺一不可。

3．三个体系

企业信息安全体系的建设最终形成三个主要体系，具体包括安全技术体系、安全管理体系以及运行保障体系。

11.1.4 信息安全体系建立的原则

企业信息安全体系的设计与建设过程，遵循了以下基本指导原则：

1．标准性原则

尽可能遵循现有的与信息安全相关的国际标准、国内标准、行业标准，包括在技术框架中与具体的信息安全技术相关的标准，以及在管理框架中与安全管理相关的标准。标准性原则从根本上保证了企业的信息安全体系建设具有良好的全面性、标准性和开放性。

2．整体性原则

从宏观的、整体的角度出发，系统地建设企业信息安全体系，不仅仅局限于安全技术层面，或者技术层面中孤立的安全技术，而是全面构架信息安全技术体系，覆盖从物理安全、通信和网络安全、主机系统安全到数据和应用系统安全各个层面。同时，建立全面有效的安全管理体系和运行保障体系，使得安全技术体系发挥最佳的保障效果。

3．实用性原则

建立信息安全体系，必须针对企业网络和信息系统的特点，在现状分析和风险评估的基础上有的放矢地进行，不能简单地照抄照搬其他的信息安全保障方案。同时，信息安全体系中的所有内容，都被用来指导企业信息安全系统的建设和管理维护等实际工作，因此必须坚持可操作性和实用性原则，避免空洞和歧义现象。

实用性还体现在信息安全体系的建设过程中，由于内容庞杂，必须坚持分步骤的有序实施原则，循序渐进地进行建设。

4．先进性原则

信息安全体系中所涉及的安全技术和机制，应该具有一定的先进性和前瞻性，既能够满足当前系统的安全要求，又能够满足未来3～5年时间内，企业的信息安全系统建设的需要，为网络和信息系统提供有效的安全服务保障。

11.1.5　信息安全策略

信息安全策略是信息安全建设的核心，它描述了在信息安全建设过程中，需要对哪些重要的信息资产进行保护，以及如何进行保护。

在对该企业进行的安全风险评估的基础之上，明确了信息安全建设工作的内容和重点，并形成了指导信息安全建设的《企业信息安全总体策略》，总体策略的设计坚持了管理与技术并重的原则，确保以网络和信息系统的安全性为主，采用多重保护、最小授权和严格管理等措施，从宏观整体的角度进行阐述，是信息安全建设总的指导原则。

按照要保障的资产对象的不同，总体策略划分为物理安全、网络安全、系统安全、病毒防治、身份认证、应用授权和访问控制、数据加密、数据备份和灾难恢复、应急响应、教育培训等若干方面进行阐述。

随着技术的发展以及系统的升级、调整，安全策略也应该进行重新评估和制定，随时保持策略与安全目标的一致性。

1. 物理安全策略

（1）计算机机房的建设必须遵循国家在计算机机房场地选择、环境安全、布线施工方面的标准，保证物理环境安全。

（2）关键应用系统的服务器主机和前置机服务器、主要的网络设备必须放置于计算机机房内部的适当位置，通过物理访问控制机制，保证这些设备自身的安全性。

（3）应当建立人员出入访问控制机制，严格控制人员出入计算机机房和其他重要安全区域，访问控制机制还需要能够提供审计功能，便于检查和分析。

（4）应当指定专门的部门和人员，负责计算机机房的建设和管理工作，建立 24h 值班制度。

（5）建立计算机机房管理制度，对设备安全管理、介质安全管理、人员出入访问控制管理等作出详细的规定。

（6）管理机构应当定期对计算机机房各项安全措施和安全管理制度的有效性和实施状况进行检查，发现问题，及时改进。

2. 网络安全策略

（1）必须对网络和信息系统进行安全域划分，建立隔离保护机制，并且在各安全域之间建立访问控制机制，杜绝发生未授权的非法访问现象，特别是必须对生产网和办公网进行划分和隔离。

（2）应当部署网络管理体系，管理网络资源和设备，实时监控网络系统的运行状态，降低网络故障带来的安全风险。

（3）应当对关键的通信线路、网络设备提供冗余设计，防止关键线路和设

备的单点故障造成通信服务中断。

（4）应当在各安全域的边界综合部署网络安全访问措施，包括防火墙、入侵检测、VPN，建立多层次的、立体的网络安全防护体系。

（5）应当建立网络弱点分析机制，发现和弥补网络中存在的安全漏洞，及时进行自我完善。

（6）应当建立远程访问机制，实现安全的远程办公和移动办公。

（7）应当指定专门的部门和人员，负责网络安全系统的规划、建设、管理和维护。

（8）应当制定网络安全系统的建设标准和相关的运营维护管理规范，在标准和规范指定的范围内指导实际的系统建设和维护管理。

（9）管理机构应当定期对网络安全措施和安全管理制度的有效性和实施状况进行检查，发现问题，及时改进。

3．系统安全策略

（1）应当对关键服务器主机设备提供冗余设计，防止单点故障造成网络服务中断。

（2）应当建立主机弱点分析机制，发现和弥补系统软件中存在的不当配置和安全漏洞，及时进行自我完善。

（3）应当建立主机系统软件版本维护机制，及时升级系统版本和补丁程序版本，保持系统软件的最新状态。

（4）应当建立主机系统软件备份和恢复机制，在灾难事件发生之后，能够快速实现系统恢复。

（5）可以建立主机入侵检测机制，发现主机系统中的异常操作行为，以及对主机发起的攻击行为，并及时向管理员报警。

（6）应当指定专门的部门和人员，负责主机系统的管理维护。

（7）应当建立主机系统管理规范，包括系统软件版本管理、主机弱点分析、主机审计日志检查和分析，以及系统软件的备份和恢复等内容。

（8）应当建立桌面系统使用管理规范，约束和指导用户使用桌面系统，并对其进行正确有效的配置和管理。

（9）管理机构应当定期对各项系统安全管理制度的有效性和实施状况进行检查，发现问题，及时改进。

4．病毒管理策略

（1）应当建立全面网络病毒查杀机制，实现企业全网范围内的病毒防治，抑制病毒的传播。

（2）所有内部网络上的计算机在联入内部网络之前，都应当安装和配置杀毒软件，并且通过管理中心进行更新，任何用户不能禁用病毒扫描和查杀功能。

（3）所有内部网络上的计算机系统都应当定期进行完整的系统扫描。

（4）从外部介质安装数据和程序之前，或安装下载的数据和程序之前，必须对其进行病毒扫描，以防止存在病毒感染操作系统和应用程序。

（5）第三方数据和程序在安装到内部网络的系统之前，必须在隔离受控的模拟系统上进行病毒扫描测试。

（6）任何内部用户不能故意制造、执行、传播、引入任何可以自我复制、破坏，或者影响计算机内存、存储介质、操作系统、应用程序的计算机代码

（7）应当指定专门的部门和人员，负责网络病毒防治系统的管理维护。

（8）应当建立网络病毒防治系统的管理规范，有效发挥病毒防治系统的安全效能。

（9）应当建立桌面系统病毒防治管理规范，约束和指导用户在桌面系统上的操作行为，以及对杀毒软件的配置和管理，达到保护桌面系统、抑制病毒传播的目的。

（10）管理机构应当定期对与病毒查杀有关安全管理制度的有效性和实施状况进行检查，发现问题，及时改进。

5．身份认证策略

（1）应当在指定范围内建立统一的用户身份管理基础设施，向应用系统提供集中的用户身份认证服务。

（2）应当选择安全性高，投入收益比例较好，易管理维护的身份认证技术，建立身份管理基础设施。

（3）每个内部员工具有指定范围内唯一的身份标识，用户在访问应用系统之前，必须提交身份标识，并对其进行认证；员工离职时，要撤销其在信息系统内部的合法身份。

（4）应当对现有的应用系统进行技术改造，使用身份管理基础设施的安全服务。

（5）应当建立专门的部门和岗位，负责用户身份的管理，以及身份管理基础设施的建设、运行、维护。

（6）应当在指定范围内建立用户标识管理规范，对用户标识格式、产生和撤销流程进行统一规定。

6．用户授权与访问控制策略

（1）应当依托身份认证基础设施，将集中管理与分布式管理有机结合起来，建立分级的用户授权与访问控制管理机制。

（2）每个内部员工在信息系统内部的操作行为必须被限定在合法授权的范围之内；员工离职时，要撤销其在信息系统内部的所有访问权限。

（3）应当对现有的应用系统进行技术改造，使用授权与访问控制系统提供的安全服务。

（4）应当建立专门岗位，负责用户权限管理，以及授权和访问控制系统的

建设、运行、维护。

（5）应当在指定范围内，建立包括用户权限的授予和撤销在内的一整套管理流程和制度。

7．数据加密策略

（1）加密技术的采用和加密机制的建立，应该符合国家有关的法律和规定。

（2）应当建立内部信息系统的密级分级标准，判定信息系统在消息传输和数据存储过程中是否需要采用加密机制。

（3）应当建立密钥管理体制，保证密钥在产生、使用、存储、传输等环节中的安全性。

（4）加密机制应当使用国际标准的密码算法，或者国内通过密码管理委员会审批的专用算法，其中对称密码算法的密钥长度不得低于 128 bit，公钥密码算法的密钥长度不得低于 1024bit。

（5）应当在物理上保证所有的硬件加密设备和软件加密程序，以及存储涉密数据的介质载体的安全。

（6）应当指定专门的管理机构，负责本策略的维护，监督本策略的实施。

（7）任何内部信息系统都需要向管理机构提出申请，经管理机构审批获得授权后，才能够使用加密机制。禁止任何内部信息系统和人员，在未授权的情况下，使用任何加密机制。

（8）管理机构应当每年对加密算法的选择范围和密钥长度的最低要求进行一次复审和评估，使得本策略与加密技术的发展相适应。

8．数据备份与灾难恢复

（1）在业务系统主要应用服务器中采用硬件冗余技术，避免硬件的单点故障导致服务中断。

（2）综合考虑性能和管理等因素，采用先进的系统和数据备份技术，在指定范围内建立统一的系统和数据备份机制，防止数据出现逻辑损坏。

（3）对业务系统采取适当的异地备份机制，使得数据备份计划具备一定的容灾能力。

（4）建立灾难恢复计划，提供灾难恢复手段，在灾难事件发生之后，快速对被破坏的信息系统进行恢复。

（5）应当建立专门岗位，负责用户权限管理，以及授权和访问控制系统的建设、运行、维护。

（6）建立日常数据备份管理制度，对备份周期和介质保管进行统一规定。

（7）建立灾难恢复计划，对人员进行灾难恢复培训，定期进行灾难恢复的模拟演练。

9．应急响应策略

（1）应当建立应急响应中心，配置专门岗位，负责制定指定范围内的信息安全策略、完成计算机网络和系统安全事件的紧急响应、及时发布安全漏洞和补丁修补程序等安全公告、进行安全系统审计数据分析以及提供安全教育和培训。

（2）应当制定详细的安全事件的应急响应计划，包括安全事件的检测、报告、分析、追查和系统恢复等内容。

10．安全教育策略

（1）应该建立专门的机构和岗位，负责安全教育与培训计划的制定和执行。

（2）应当制定详细的安全教育和培训计划，对信息安全技术和管理相关人员进行安全专业知识和技能培训，对普通用户进行安全基础知识、安全策略和管理制度培训，提高人员的整体安全意识和安全操作水平。

（3）管理机构应当定期对安全教育和培训的成果进行抽查和考核，检验安全教育和培训活动的效果。

11.1.6　信息安全体系框架

企业进行信息安全建设的目标是建立起一个全面、有效的信息安全体系，在这个体系中，包括了安全技术、安全管理、人员组织、教育培训、资金投入等关键因素，信息安全建设的内容多，规模大，必须进行全面的统筹规划，明确信息安全建设的工作内容、技术标准、组织机构、管理规范、人员岗位配备、实施步骤、资金投入，才能够保证信息安全建设有序可控地进行，才能够使得信息安全体系发挥最优的保障效果。

为此制定了《企业信息安全体系框架》，该框架主体由“综述”、“安全技术框架”、“安全管理框架”、“运营保障框架”、“建设实施规划”五部分组成，从宏观上规划和管理信息安全建设工作。

同时还制定了“企业信息安全管理规范汇编”，包括了一系列的安全管理规范，指导信息安全建设和运营工作，使得信息安全建设能够依据统一的标准开展，信息安全体系的运营和维护能够遵循统一的规范进行。

1．安全目标模型

根据企业信息安全体系建设目标和总体安全策略，建立了与之对应的目标模型，称为 WP^{2}DRR 安全模型，该模型是基于时间的，由预警（Warning）、策略（Policy）、保护（Protection）、检测（Detection）、响应（Response）、恢复（Recovery）六个要素环节构成了一个完整的、动态的信息安全体系，如图 11-2 所示。预警、保护、检测、响应、恢复等环节都由技术内容和管理内容所构成。

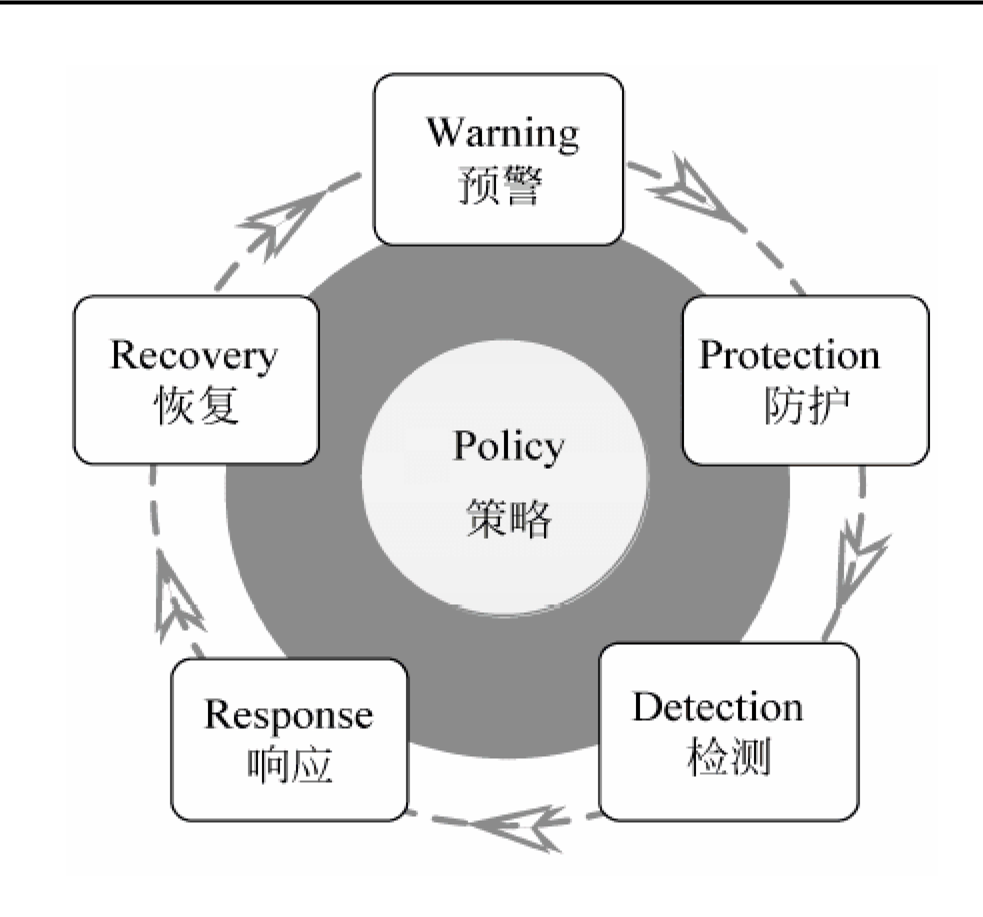


图 11-2　WP^2DRR 安全模型

（1）Policy（安全策略）：根据风险分析和评估产生的安全策略描述了系统中哪些资源要得到保护，以及如何实现对它们的保护等。在 WP^2DRR 安全模型中，策略处于核心地位，所有的防护、检测、响应、恢复都依据安全策略展开实施，安全策略为安全管理提供管理方向和支持手段。

（2）Warining（预警）：根据以前所掌握的系统弱点和当前了解的犯罪趋势预测未来可能受到的攻击和危害，包括风险分析、病毒预报、黑客入侵趋势预报和情况通报、系统弱点报告和补丁到位。

（3）Protection（防护）：通过修复系统漏洞、正确设计开发和安装安全系统来预防安全事件的发生；通过定期检查来发现可能存在的系统弱点；通过教育等手段，使用户和操作员正确使用系统，防止意外威胁；通过访问控制、监控等手段来防止恶意威胁。

（4）Detection（检测）：检测是非常重要的一个环节，检测是动态响应和加强防护的依据，它也是强制落实安全策略的有力工具，通过检测和监控网络及信息系统，发现新的威胁和弱点，通过循环反馈来及时作出有效的响应。

（5）Response（响应）：响应是对安全事件作出反应，包括对检测到的系统异常或者攻击行为作出响应动作，以及处理突发的安全事件。恰当的响应动作和响应流程可以降低安全事件的不良影响，加强对重要资源的保护。

（6）Recovery（恢复）：灾难恢复能力直接决定了业务应用的持续可用性，任何意外的突发事件都可能造成服务中断和数据受损，优秀的灾难恢复计划能够针对灾难事件做到未雨绸缪，即使系统和数据遭受破坏，也能够在最短的时间内完成恢复操作。

WP^2DRR 安全模型的特点就是动态性和基于时间的特性。它阐述了这样一个结论：安全的目标实际上就是尽可能地增大保护时间，尽量减少检测时间和响应时间。

WP^2DRR 模型是在传统的 P^2DR 模型的基础上新增加了预警 Warning 和恢复 Recover，增强了安全保障体系的事前预防和事后恢复能力，一旦系统安全

事故发生了，也能恢复系统功能和数据，恢复系统的正常运行。

安全目标模型是信息安全体系框架的基础，企业的信息安全体系框架紧密围绕这个安全模型的六个要素环节进行设计，每个要素环节的功能都在安全技术体系、安全组织和管理体系以及运行保障体系中体现出来。

2. 信息安全体系框架组成

通过对企业的网络和应用现状、安全现状、面临的安全风险的分析，根据安全保障目标模型，制定了企业信息安全体系框架，制定该框架的目的在于从宏观上指导和管理信息安全体系的建设和运营。

该框架由一组相互关联、相互作用、相互弥补、相互推动、相互依赖、不可分割的信息安全保障要素组成。一个系统的、完整的、有机的信息安全体系的作用力远远大于各个信息安全保障要素的保障能力之和。在此框架中，以安全策略为指导，融会了安全技术、安全管理和运行保障三个层次的安全体系，达到系统可用性、可控性、抗攻击性、完整性、保密性的安全目标。

企业信息安全体系框架的总体结构如图 11-3 所示。

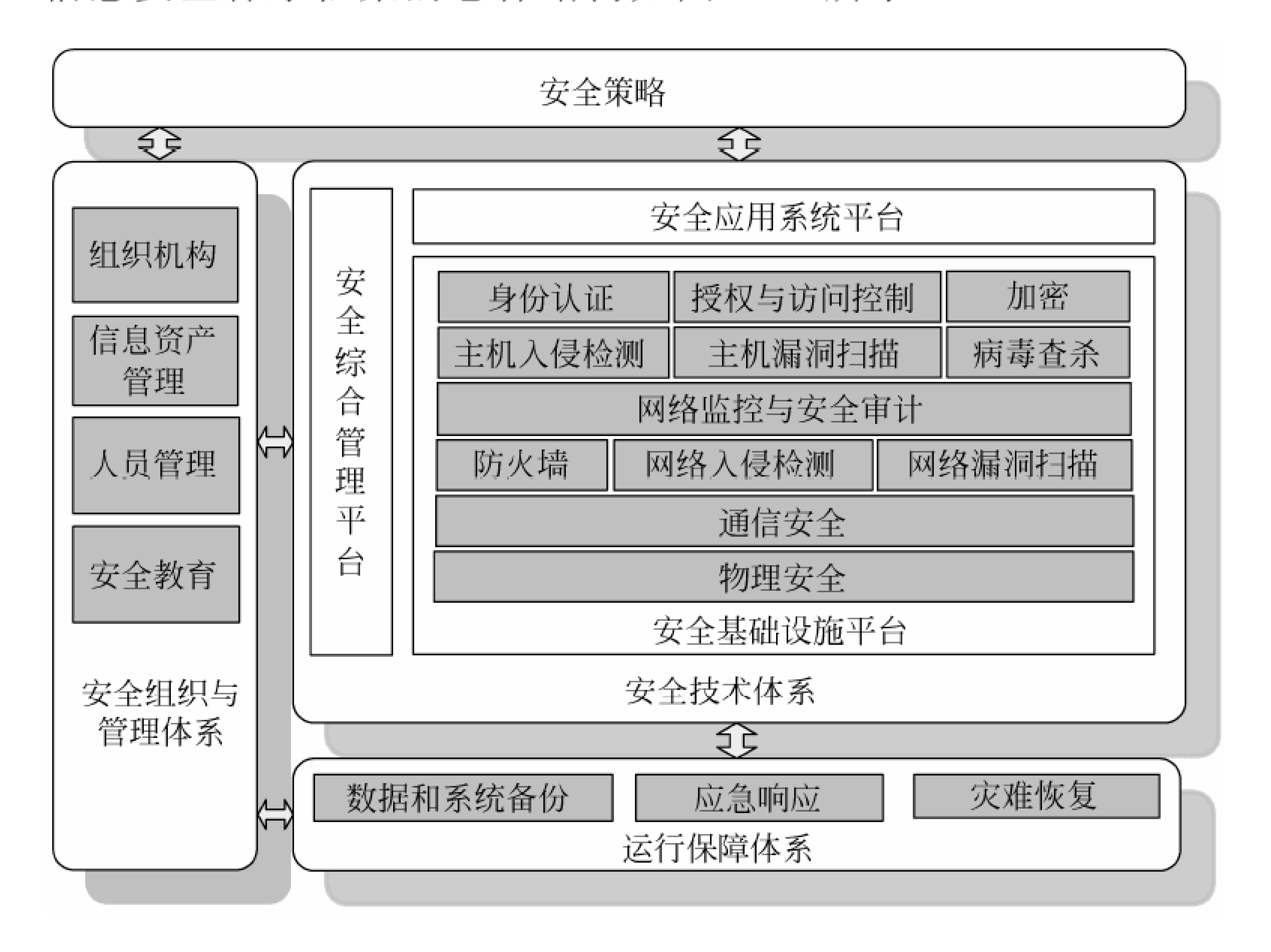


图 11-3　企业信息安全体系框架

1）安全策略

在这个框架中，安全策略是指导。安全策略与安全技术体系、安全组织和管理体系以及运行保障体系这三大体系之间的关系也是相互作用的。一方面，三大体系是在安全策略的指导下构建的，主要是将安全策略中制定的各个要素转化成为可行的技术实现方法和管理、运行保障手段，全面实现安全策略中所制定的目标；另一方面，安全策略本身也有包括草案设计、评审、实施、培训、

部署、监控、强化、重新评估、修订等步骤在内的生命周期，需要采用一些技术方法和管理手段进行管理，保证安全策略的及时性和有效性。

2）安全技术体系

安全技术体系是整个信息安全体系框架的基础，包括了安全基础设施平台、安全应用系统平台和安全综合管理平台三个部分，以统一的信息安全基础设施平台为支撑，以统一的安全系统应用平台为辅助，是在统一的综合安全管理平台管理下的技术保障体系框架。

安全基础设施平台是以安全策略为指导，从物理和通信安全防护、网络安全防护、主机系统安全防护、应用安全防护等多个层次出发，立足于现有的成熟安全技术和安全机制，建立起的一个各个部分相互协同的完整的安全技术防护体系。

安全应用系统平台处理安全基础设施与应用信息系统之间的关联和集成问题，应用信息系统通过使用安全基础设施平台所提供的各类安全服务，提升自身的安全等级，以更加安全的方式提供金融业务服务和内部信息管理服务。

安全综合管理平台的管理范围尽可能地涵盖安全技术体系中涉及的各种安全机制与安全设备，对这些安全机制和安全设备进行统一的管理和控制，负责管理和维护安全策略，配置管理相应的安全机制，确保这些安全技术与设施能够按照设计的要求协同运作，可靠运行。它在传统的信息系统应用体系与各类安全技术、安全产品、安全防御措施等安全手段之间搭起桥梁，使得各类安全手段能与现有的信息系统应用体系紧密的结合实现无链链接，促成信息系统安全与信息系统应用的真正一体化，使得传统的信息系统应用体系逐步过渡到安全的信息系统应用体系。

统一的安全管理平台有助于各种安全管理技术手段的相互补充和有效发挥，也便于从系统整体的角度来进行安全的监控和管理，从而提高安全管理工作的效率，使人为的安全管理活动参与量大幅下降。

3）安全管理体系

安全组织和管理体系是安全技术体系真正有效发挥保护作用的重要保障，安全管理体系的设计立足于总体安全策略，并与安全技术体系相互配合，增强技术防护体系的效率和效果，同时也弥补当前技术无法完全解决的安全缺陷。

技术和管理是相互结合的，一方面安全防护技术措施需要安全管理措施来加强，另一方面技术也是对管理措施贯彻执行的监督手段。在企业信息安全体系框架中，安全管理体系的设计充分参考和借鉴了国际信息安全管理标准 BS 7799（ISO 17799）的建议和国家《银行及相关金融服务信息安全管理规范》的要求。

企业信息安全管理体系由若干信息安全管理类组成，每项信息安全管理类可分解为多个安全目标和安全控制。每个安全目标都有若干安全控制与其相对应，这些安全控制是为了达成相应安全目标的管理工作和要求。信息安全管理体系一共包括了以下 12 项管理类：

（1）安全策略与制度：确保企业拥有明确的信息安全方针以及配套的策略

和制度，以实现对信息安全工作的支持和承诺，保证信息安全的资金投入。

（2）安全风险管理：信息安全建设不是避免风险的过程，而是管理风险的过程。没有绝对的安全，风险总是存在的。信息安全体系建设的目标就是要把风险控制在可以接受的范围之内。风险管理同时也是一个动态持续的过程。

（3）人员和组织安全管理：建立组织机构，明确人员岗位职责，提供安全教育和培训，对第三方人员进行管理，协调信息安全监管部门与行内其他部门之间的关系，保证信息安全工作的人力资源要求，避免由于人员和组织上的错误产生的信息安全风险。

（4）环境与设备安全管理：控制由于物理环境和硬件设施的不当所产生的风险。管理内容包括物理环境安全、设备安全、介质安全等。

（5）网络与通信安全管理：控制和保护网络和通信系统，防止其受到破坏和滥用，避免和降低由于网络和通信系统的问题对企业金融业务系统的损害。

（6）主机与系统安全管理：控制和保护企业的计算机主机及其系统，防止其受到破坏和滥用，避免和降低由此对金融业务系统的损害。

（7）应用与业务安全管理：对各类应用和业务系统进行安全管理，防止其受到破坏和滥用。

（8）数据安全和加密管理：采用数据加密和完整性保护机制，防止数据被窃取和篡改，保护银行业务数据的安全。

（9）项目工程安全管理：保护信息系统项目工程过程的安全，确保项目的成果是可靠的安全系统。

（10）运行和维护安全管理：保护信息系统在运行期间的安全，并确保系统维护工作的安全。

（11）业务连续性管理：通过设计和执行业务连续性计划，确保信息系统在任何灾难和攻击下，都能够保证业务的连续性。

（12）合规性（符合性）管理：确保企业的信息安全保障工作符合国家法律、法规的要求，并且企业的信息安全方针、规定和标准得到了遵循。

12 项信息安全管理类之间的关系，如图 11-4 所示。

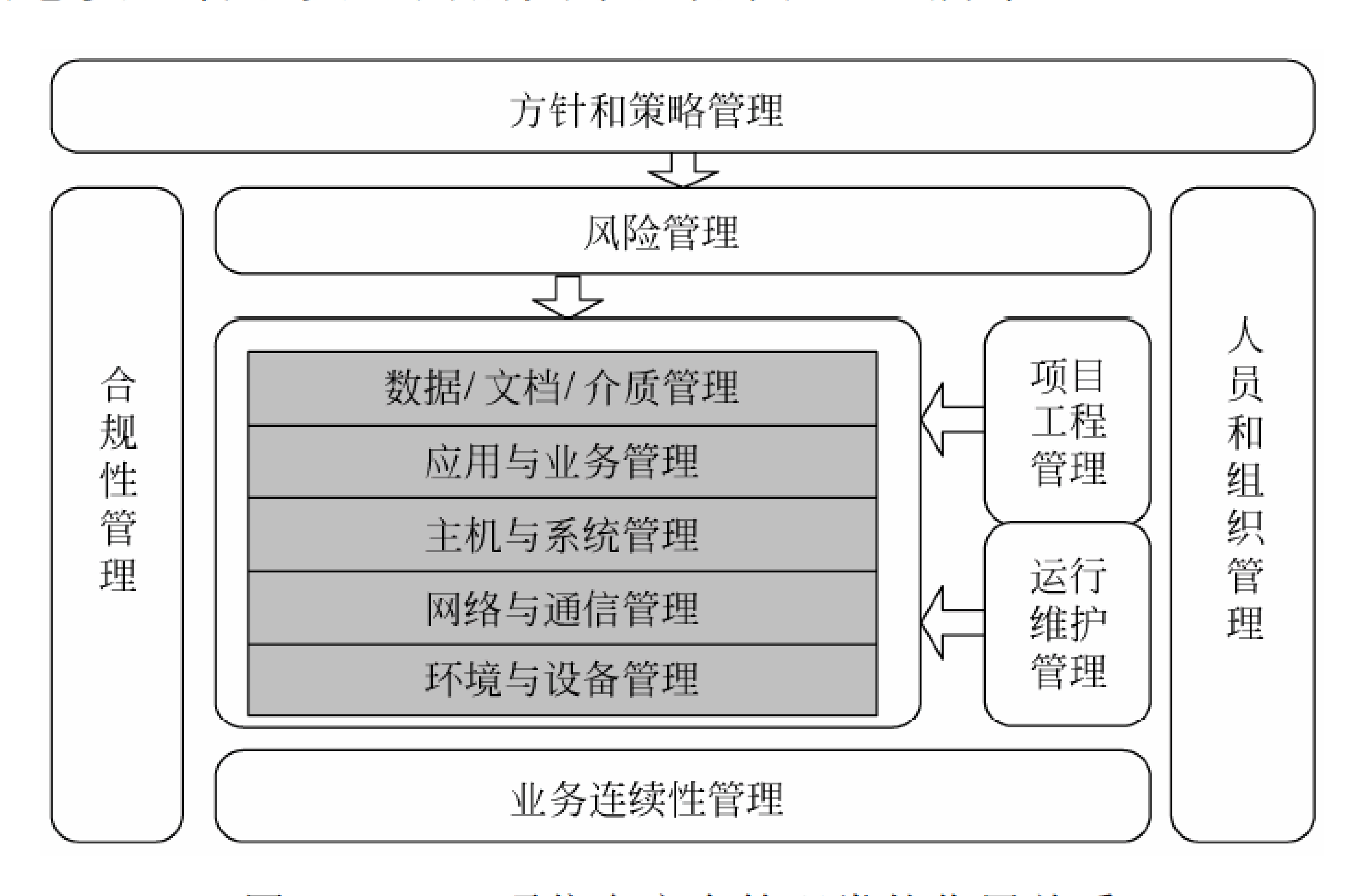


图 11-4 12 项信息安全管理类的作用关系

12 项信息安全管理类的作用关系如下：

（1）方针和策略是企业整个信息安全管理工作的基础和整体指导，对于其他所有的信息安全管理类都有指导和约束关系。

（2）人员和组织管理要依据方针和策略来执行信息安全管理工作。

（3）合规性指导如何检验信息安全管理工作的效果，特别是对于国家法律法规、方针政策和标准符合程度的检验。

（4）根据“方针和策略”，由“人员和组织”实施信息安全管理工作。在实施中主要从两个角度来考虑问题，即风险管理和业务连续性管理。

（5）根据信息系统的生命周期，可以将信息系统划分为两个阶段，即项目工程开发阶段和运行维护阶段。这两个信息安全管理类体现了信息系统和信息安全工作的生命周期特性。

（6）最终所有的信息安全管理工作都作用在信息系统之上。信息系统可以划分成五个层次，从底层到上层依次为环境与设备管理、网络与通信管理、主机与系统管理、应用与业务管理、数据/文档/介质管理。这五个信息安全管理类体现了信息系统和信息安全工作的层次性。

4）运行保障体系

运行保障体系由安全技术和安全管理紧密结合的内容所组成，包括了系统可靠性设计、系统数据的备份计划、安全事件的应急响应计划、安全审计、灾难恢复计划等，运行和保障体系对于企业网络和信息系统的可持续性运营提供了重要的保障手段。

5）建设实施规划

建设实施规划是在安全管理体系、安全技术体系、运行保障体系设计的基础上进一步制定的建设步骤和实施方案。在建设实施规划中突出体现了分步有序实施的原则。

任何信息安全建设都需要人员负责管理和实施，因此，首先应该建立信息安全工作监管组织机构，明确各级管理机构的人员配备、职能和责任。其中信息安全管理机构负责信息安全策略的审核与颁布、统一技术标准和管理规范的制定、指导和监督信息安全建设工作、对信息安全系统进行监控与审计管理。

信息安全体系建设，应该首先从物理环境安全建设入手，确保机房建设按照统一的标准进行，并且按照统一的管理规范进行管理。

接下来应该进行网络安全建设，应该对计算机网络的安全域进行划分，对网络结构进行调整，确保内部网络与外部网络、业务网络与办公网络边界清晰；在各安全域的边界处部署防火墙、网络入侵检测等安全产品，形成立体的区域边界保护机制，对各安全域进行逻辑安全隔离，禁止未授权的网络访问；在内部网络中部署网络脆弱性分析工具，定期对内部网络进行检查，并采取措施及

时弥补新发现的安全漏洞。

在进行网络安全建设的同时，可以进行系统安全建设，在内部网络中全面部署网络病毒查杀系统，有效抑制计算机病毒在内部网络中传播，避免对系统和数据造成损害；另外，主机系统管理员还应该按照主机系统管理规范的要求，借助主机脆弱性分析和安全加固工具，定期对主机系统进行检查，更新安全漏洞补丁的级别，修正不当的系统和服务配置，查看和分析系统审计日志，控制和保证主机系统的良好安全状态。

应用安全建设包括建立身份认证系统、应用授权和访问控制系统、数据安全传输系统等，对金融业务应用系统和内部信息管理系统提供各种安全服务。

按照统一的标准，建立安全审计与分析系统、系统和数据备份计划、安全事件应急响应计划、灾难恢复计划等安全保障机制，重在保护业务数据等信息资产，保证内外应用服务的持续可用性。

对所有员工进行基本安全教育，为信息安全系统相关技术人员提供专门的安全理论和安全技能培训，提高全员的安全意识，打造一支高素质的专业技术和管理队伍。

11.2　信息安全规划管理案例

11.2.1　项目背景

随着银行业务的快速发展，对于信息科技的依赖程度越来越强，致使信息科技风险不断加大，即使短暂的运行异常也将影响到大量的客户，会对银行的效益和整体声誉产生严重影响。另一方面，信息系统规模的剧增也使得内在对象之间的依赖关系错综复杂，基础环节的问题很有可能引发系统性的故障。为更好地履行企业公众责任和壮大企业业务能力，需要开展信息科技风险管理工作，有效地预防、控制和转移风险，确保信息科技对业务的可靠支撑，全面提升银行的核心竞争力。及时发现和了解现有信息科技管理和运营的潜在风险并采取积极的措施进行应对，建立有效、完整的信息科技风险控制体系，是银行在当前经济环境中生存和发展的必要条件。

11.2.2　项目实施目标

落实监管机构要求，建立有效的信息科技风险管理机制，识别风险，完善制度，实现银行信息科技风险管理工作规范化、常规化，形成长效机制，具体如图 11-5 所示。

1

◆对银行信息科技风险管控现状进行评估，识别出需要关注的风险并制定其应对方案、实施计划，通过实施具体的风险管控措施（包括管理制度的完善及技术措施的优化和增强），有效地预防、控制和转移风险，降低信息科技风险水平。

2

◆实现对银行信息科技风险的识别、计量、检测和控制，确保信息科技对业务的可靠支撑，促进银行信息科技安全、持续、稳健运行，增强核心竞争力和可持续发展能力。

3

◆结合信息科技风险管理框架、策略、制度、标准的制订，推出强化信息科技风险管理工作的行动措施，形成银行信息科技风险管控体系，提升自身风险管控能力和水平，最终符合《商业银行信息科技风险管理指引》的各项要求。

图 11-5 项目实施目标

11.2.3 项目工作内容

（1）根据中国银监会《商业银行信息科技风险管理指引》（以下简称《指引》）并结合银行实际，进行信息科技风险评估，完成评估报告。评估报告至少包括四个方面：确定评估的方法和工具；分析信息科技活动领域及管理的信息科技风险类型与分布环节，找出信息科技风险点（固有风险），形成信息科技风险点库；分析评估信息科技风险状况，包括控制措施的有效性、剩余风险状况等级及是否在银行可承受的范围内等；提出关键岗位信息科技员工流失风险评估方法，并分析评估自 2008 年至今信息科技员工流失带来的风险。

（2）进行信息科技风险管理工作的差异分析并形成报告。根据《指引》要求和银行实际，进行至少三个方面的分析：分析监管法规对各类风险管理提出的具体要求；分析评估制度与监管要求的差异；分析评估信息科技风险管理现状与监管要求及制度之间的差异。

（3）根据银行信息科技风险管理和控制框架建议方案，提出参考性的银行信息科技风险管理策略。

（4）根据《指引》要求和银行实际，对信息科技制度、流程进行梳理，找出管理流程中存在的风险点，从防范风险、提高效率的角度提出优化流程和加强制度控制措施的建议，提出信息科技风险管理制度体系建议方案；形成信息科技风险管理工作旧制度体系框架、制度名录以及信息科技风险管理工作新制度体系框架、制度名录，以及完成所有科技类制度的制订、修订、优化、精简等工作，包括相应的执行流程等；完成信息安全技术管理标准的制定；完成信息科技重要岗位工作手册的制定。

（5）就强化信息科技风险管理工作提出建议行动措施、计划或规划。

（6）进行年度信息科技风险评估和《指引》落实效果的首次评估验收。

（7）以专门的交流和培训等方式实现对评估知识、方法、技术和工具等的知识转移和团队培养。

11.2.4　项目实施方法

1. 信息科技现状风险评估

依据监管机构要求，以《指引》为主，同时借鉴 ISO 27001、COBIT、COSO、ITIL、国家信息安全等级保护要求、财政部《企业内部控制规范》等国内外相关标准与金融业最佳实践，结合银行实际，形成银行信息科技风险评估指标体系。信息科技风险评估指标体系涵盖以下方面：信息科技治理，信息科技风险管理，信息安全，信息系统开发，测试和维护，信息科技运行，业务连续性管理，外包，内部审计，外部审计。提出关键岗位信息科技员工流失风险评估方法，并分析评估自 2008 年至今信息科技员工流失带来的风险。

开展信息科技整体风险评估，包括管理、技术等方面，梳理并分类描述信息科技工作的主要活动领域及其工作流程，根据科技工作的活动事项，划分相应的风险类型、表现形式及其分布环节，分析各类主要风险的潜在影响并进行风险分级。风险分级按照风险程度（高、低）和发生频率（高、低）进行分级与排序，形成银行信息科技整体风险评估报告。

2. 管理差异分析

按照综合风险、各分类风险管理领域，梳理分析监管法规对信息科技风险管理提出的具体要求，形成信息科技监管法规要求汇编。《信息科技监管法规要求汇编》包括国家、部委、人民银行、银监会等全部现行的信息科技管理相关法律、法规、制度、通知等。

依据监管机构法规要求，以《指引》为主，按照综合风险、各分类风险管理领域，分析银行已实施的风险管理规划、策略、制度、政策、措施及风险防范效果，对比监管要求和银行现行制度，分析并提出银行制度与监管要求的差异，将管理现状与监管要求、银行制度规范进行对比，分别分析并提出管理现状与监管法规要求、管理现状与银行制度规范的差异。

3. 信息科技风险管理策略制定

结合国际信息科技风险管理标准，依据人民银行、银监会、国家信息安全等级保护要求设计银行信息科技风险控制策略框架，内容包括《指引》要求，设计适合银行的信息科技风险控制框架，并制定信息科技风险管理策略，至少包括《网上银行系统信息安全规范》（2010 年人行 19 号文）中的以下方面：

（1）信息分级与保护；

（2）信息系统开发、测试和维护；

（3）信息科技运行和维护；
（4）访问控制；
（5）物理安全；
（6）人员安全；
（7）业务连续性计划与应急处置；
（8）安全制度管理；
（9）信息安全组织管理；
（10）资产管理；
（11）人员安全管理；
（12）物理与环境安全管理；
（13）通信与运营管理；
（14）访问控制管理；
（15）系统开发与维护管理；
（16）信息安全事故管理；
（17）业务连续性管理；
（18）合规性管理；
（19）知识产权管理。

4．制定制度体系框架、制度名目及信息科技风险管理行动措施

以《银行信息科技风险管理现有制度类文件清单》、《银行信息科技风险管理通知要求类文件清单》为基础，进一步进行全面梳理，形成银行信息科技风险管理工作旧制度体系框架、制度名录；构建银行信息科技管理新的制度体系框架，充分考虑制度间的关联关系，制定新的制度体系框架下的制度名录。

根据风险评估报告、管理差异分析报告和信息科技风险管理策略，通过对银行现状及已经完成工作的阶段性总结，针对银行各相关单位，制定信息科技风险管理行动措施建议，其中包含信息科技风险相关的机构岗位职责建议和各岗位应具有的专业知识和技能。配合银行各相关单位，结合各自实际工作，制定细化的信息科技风险管理工作计划。

5．制度重整

根据新的制度名录，优化、完善信息科技管理制度。完成新制度制定，现有制度的修订完善、内容规范、重新组合等，其中包括相应的执行流程。制度制订、修订、优化、精简等的基本标准和纲领是《指引》的各项要求，信息科技管理制度涵盖信息科技治理，信息科技风险管理，信息安全，信息系统开发，测试和维护，信息科技运行，业务连续性管理，外包，内部审计，外部审计九个方面，包括信息科技组织管理、培训、报告、风险管理、风险评估管理、风险计量监测、信息安全管理、信息系统检查管理、用户认证和访问控制、网络安全、操作系统管理、生产系统日志管理、加密管理、设备管理、数据安全、

项目管理、规划管理、需求管理、软件开发管理、测试管理、变更管理、问题缺陷管理、版本管理、质量管理、运行管理、机房管理、软硬件运行维护、网络运行维护、监控、应急管理及处置、外包管理、审计管理等内容。信息安全技术管理标准制定，包括物理安全、网络安全、主机安全、应用安全、数据安全等方面。信息科技重要岗位工作手册制定，包括岗位职责、工作流程、岗位知识和技能等内容。

6. 年度信息科技整体风险评估

对总行和各分行进行全面的信息科技风险评估，并涵盖技术系统之间、总分行之间、部门之间、分行之间、制度之间等领域，编写信息科技整体风险评估报告。

7.《指引》贯彻落实效果评估

制定信息科技风险评估规范，形成风险评估的方法、流程、模型、工具和评价指标体系。实现对《指引》涉及的 19 个方面要求内容的分拣和归类，形成银行今后内、外审依据。需要编写信息科技风险评估规范和信息科技风险评估标准，开发信息科技风险评估系统，支撑银行信息科技风险评估的常规化工作开展。

针对项目前期的实施成果，组织相关人员进行培训，通过培训等形式进行知识转移与团队培养。

根据《指引》要求，使用前期形成的信息科技风险评估规范、方法、流程、模型、工具和指标体系，评价银行贯彻落实情况，形成《<指引>落实情况报告》。

11.3　信息安全运维实践案例

11.3.1　项目背景

经过多年的实践，企业集团已形成了一整套具有集团特色的管理制度和模式，并取得了较好的成绩。随着产业、科技、成套装备、物流贸易等业务的不断发展，以及“国际化”战略的实施，集团业务规模不断扩大。企业集团充分认识到信息化对提高集团整体运营效率和核心竞争力的战略作用，高度重视集团信息化建设，通过信息化建设不断促进管理创新，集团信息系统数量大幅增加，系统复杂程度大幅提高，业务依赖程度大幅增强，特别是集团的基础信息网络和重要信息系统已经成为支撑集团业务发展的重要保证。

11.3.2　项目目标

（1）明确集团内省中心各业务系统及地市日常安全工作的基本内容，加强

网络安全的例行作业，切实落实网络安全的预防性管理。

（2）为确保高效准确执行日常安全工作，本工作规范制定各项安全工作的制度、执行流程，指导日常安全工作的开展，为各级安全负责人员提供基础工作指引和操作规程。

（3）通过日常安全工作的执行，充分发挥网络中安全防护产品和措施的作用，确保网络和业务系统正常、稳定地运行。

（4）通过本工作规范的执行和落实，加强安全防护体系中人员、组织及管理制度的完善和建立。

（5）工作规范适用于集团责任公司省中心、各地市公司的网管系统、业务支撑系统和企业信息网等系统的基础安全工作。

11.3.3 项目工作内容

1. 安全现状分析

根据调研访谈结果以及各地市反馈的调查表，目前省中心和各地市的安全工作现状如下：

（1）省公司和地市公司的日常安全工作中包括以下内容：

① 系统安全管理，包括系统软件与补丁管理、日常防病毒管理、安全产品策略备份等；

② 账号、口令管理，包括账号管理、密码管理；

③ 安全审计管理，包括定期系统扫描、日志审计管理。

（2）省公司和地市公司希望在今后的安全工作中应完善和加强以下工作内容：

① 各系统的账号的权限管理和控制；

② 新入网系统安全检查；

③ 安全事件流程管理。

（3）目前的网络安全工作与系统维护工作结合在一起，虽然维护工作职责中包含和描述了安全工作的相关内容，但是没有明确规定安全工作内容、工作规范、工作标准等，因此目前的安全基础工作主要依赖于维护人员经验。

（4）目前，省公司、地市公司各业务系统由系统管理人员兼职完成日常安全工作。

（5）目前，省公司、地市公司各业务系统在日常安全工作中执行的安全管理制度，需要加强其执行能力。

2. 安全日常工作内容

针对现有情况分析，将网络安全日常工作分为五类内容，即安全日常管理、账号和口令管理、周期性审计管理、新入网系统安全检查和安全事件管理。

（1）安全日常管理：对目前网络和系统中部署的安全措施进行日常维护，

检查安全产品运行状态，保证安全产品和措施能够发挥安全防护作用。

（2）账号和口令管理：完成各种账号创建、账号删除等维护管理功能；定期对账号进行检查；加强对第三方维护人员进行账号管理；定期清理长期不用和不合理的用户。

（3）周期性审计管理：定期利用漏洞扫描工具对各指定的服务器和终端进行扫描，跟踪系统的配置安全和漏洞检查；定期对安全工作的相关文档进行检查，进行备份。

（4）新入网系统安全检查：对新接入的系统利用漏洞扫描工具对各指定的服务器和终端进行扫描，确保新接入系统不会给现有网络带来威胁。

（5）安全事件管理：对于网络中的各种安全事件定义危险级别，制定各级安全事件处理流程以及应急体系，建立安全事件处理的知识库。

3. 安全日常工作组织分工及角色职责

安全日常工作标准指导省中心网管系统、业务支撑系统、OA 系统，以及地市各分公司网管系统、业务支撑系统、OA 系统的管理维护人员进行日常安全管理工作。

省公司网络部是标准的制定者，对标准具有最终解释权，在省中心其他部门以及地市的日常安全维护工作中给予解释和支持。在每年的安全巡检工作中，根据本规范进行安全工作的检查。

省公司网管中心、业务支撑中心和企业信息中心以及地市分公司的网管维护中心和信息技术中心的工作人员执行本标准，完成日常安全基础工作。

在省公司网管中心、业务支撑中心和企业信息中心以及地市分公司的网管维护中心和信息技术中心负责安全工作的人员分为：安全监控人员、安全管理人员、系统管理人员、各科室领导等角色。具体每个角色的职能如下：

（1）安全监控人员：主要负责安全产品的运行状态检查，通过安全产品的管理中心搜集各种安全告警。

（2）安全管理人员：主要负责安全产品配置、维护、升级和管理；安全事件的处理；对于重大的安全事件协调厂商完成处理工作；完成对各项安全工作的周期性检查等工作。

（3）系统管理人员：负责各系统维护工作，协助完成安全管理工作。

（4）各科室领导：负责各种账号申请的审批，各种安全策略调整的审批；指导安全事件的处理；对各项安全工作进行周期性检查。

4. 网络安全维护工作

网络安全维护工作是指对目前网络和系统中部署的安全措施进行日常维护，检查安全产品运行状态，保证安全产品和措施能够发挥安全防护作用。其具体包括防火墙管理、入侵检测系统管理、防病毒服务器管理和补丁管理等。

1）防火墙管理

（1）防火墙的运行状况定期检查包括：

工作内容：定期检查防火墙的运行状况，保证防火墙正常运行；定期检查防火墙是否正常生成日志信息。

工作频率：每天。

工作时间：1h 左右。

工作角色：安全监控人员。

需要执行流程：安全预警处理流程、严重安全事件处理流程、一般安全事件处理流程

防火墙运行状况检查详细工作内容：

- 安全监控人员每天检查防火墙的 CPU 利用率、连接数情况，填写“防火墙日常安全检查表”；
- 如果发现 CPU 使用量和连接数超过防火墙性能的 70%以上，上报给安全管理人员，根据“安全预警处理流程”处理；
- 如果发现防火墙发生故障，不能正常工作，根据“严重安全事件处理流程”处理；
- 安全监控人员每天检查防火墙日志是否正常记录，填写“防火墙日常安全检查表”；
- 如果防火墙日志记录不成功，上报给安全管理人员，根据“一般安全事件处理流程”处理。

说明：表 11-1 中的信息仅供参考，各业务系统根据实际情况增加其他项目，并且制定各系统的标准。

表 11-1 防火墙日常安全检查表

防火墙日常安全检查表				
值班人员		日期		
设备名称		系统管理员		
所属科室		所属系统		
检查项目	子项	检查结果		备注
系统运行情况	CPU 利用率			
	内存利用率			
	系统连接数			
	是否正常工作	正常/不正常		
日志检查	是否生成昨天的日志	正常/不正常		
	是否记录当时的日志	正常/不正常		

（2）定期备份防火墙生成日志信息包括：

工作内容：定期对防火墙日志进行备份，并进行集中存档。

工作频率：每周一。

工作时间：1h。

工作角色：安全管理人员。

需要记录表格：无。

定期备份防火墙生成日志详细工作：安全管理人员每周一定时对防火墙日志进行备份，以“防火墙名＋当天的日期”命名文件并集中存档。

（3）遵守流程进行防火墙策略调整包括：

工作内容：定期对防火墙日志进行备份，并进行集中存档。

工作频率：无。

工作角色：安全管理人员。

调整防火墙策略详细工作：

- ❑ 本项工作不属于日常值班人员工作范围，不需要安全监控人员填写；
- ❑ 本申请单需要经过室经理、业务系统管理人员审批后，才可进行防火墙策略调整；
- ❑ 首先由申请人员填写防火墙策略申请单，然后遵守“防火墙配置修改流程”对防火墙配置进行修改，详见工作流程；
- ❑ 在修改防火墙配置前、后必须备份当时的配置信息，并以“防火墙名称＋当天日期＋备份时间”进行命名，并归档保存。

防火墙配置修改流程如图 11-6 所示。

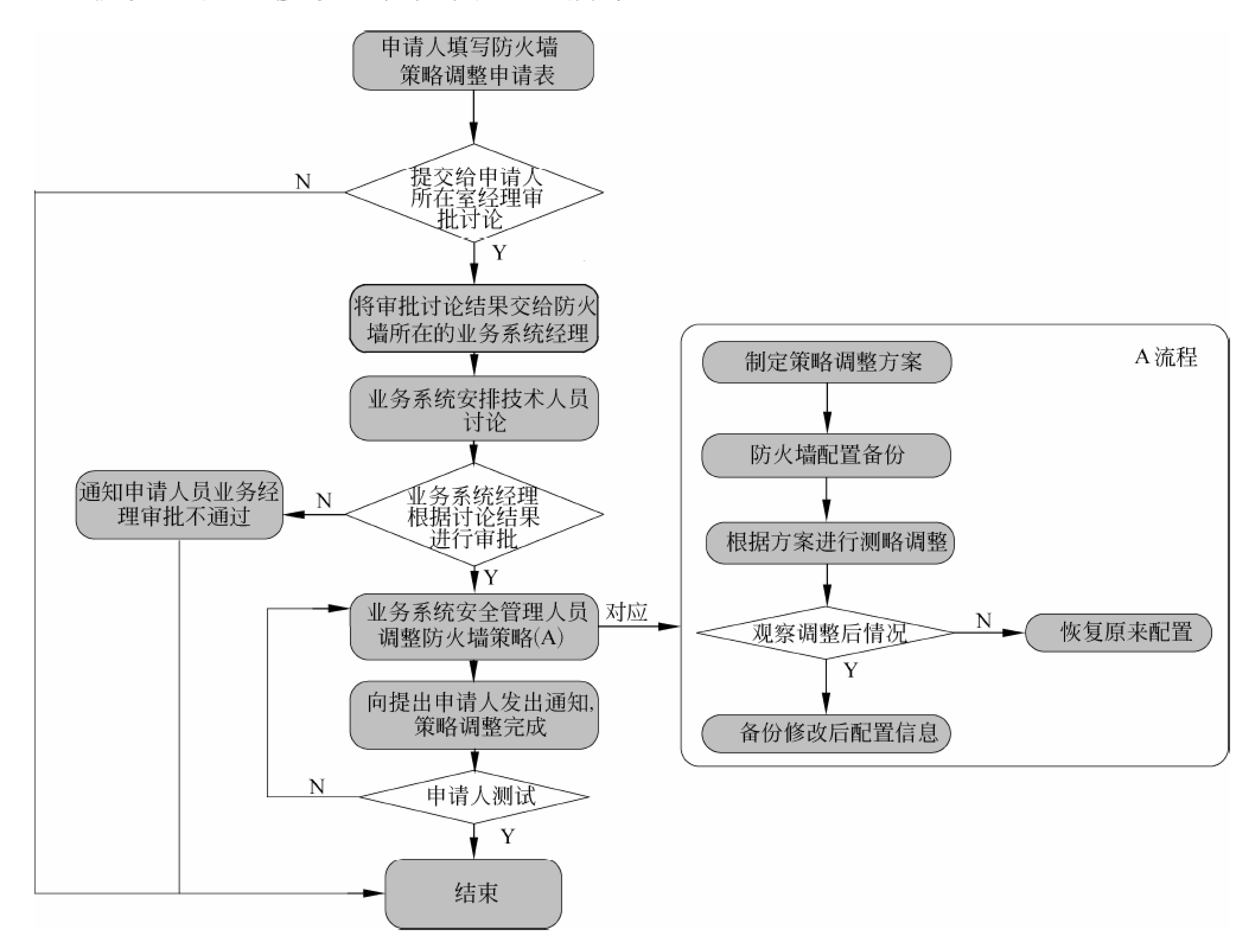


图 11-6　防火墙配置修改流程

2）入侵检测系统管理

（1）入侵检测系统的运行状况定期检查包括：

工作内容：定期检查入侵检测系统的运行状况，保证其正常运行；定期检查入侵检测系统是否正常生成告警信息。

工作频率：每天。

工作时间：1h。

工作角色：安全监控人员。

入侵检测系统的运行状况定期检查详细工作：

- 安全监控人员每天检查网络 IDS 的控制中心是否正在运行，引擎是否正常工作，将检测结果填写“IDS 日常安全检查表”（见表 11-2）；
- 安全监控人员检查网络 IDS 的引擎与控制台是否连接，将检测结果填写“IDS 日常安全检查表”；
- 如果控制中心和引擎连接不正常，上报到安全管理人员，根据“一般安全事件处理流程”进行解决；
- 安全监控人员每天检查网络 IDS 的显示中心是否实时进行告警显示，将检测结果填写“IDS 日常安全检查表”；
- 如果不能实时显示告警，上报安全管理人员，根据“一般安全事件处理流程”进行解决；
- 安全监控人员测试控制中心与数据库是否连接正常，填写“IDS 日常安全检查表”；
- 如果控制中心与数据库连接不正常，上报安全管理人员，根据“一般安全事件处理流程”处理；
- 当告警日志存储造成服务器硬盘空间不足 5GB 时，应及时进行处理，处理措施包括异地备份或删除。

表 11-2 IDS 日常安全检查表

防火墙日常安全检查表				
值班人员		值班日期		
设备名称		所属系统		
所属科室		系统管理人员		
检查项目	检查子项	标准	检查结果	备注
系统运行状况	控制中心是否正在运行	系统没有出现错误提示，能正常操作		
	引擎与控制台是否正常连接	控制中心显示与引擎处于正常连接状态		
是否产生实时告警	显示中心是否进行实时告警	显示中心是否实时出现告警信息		
	测试控制中心与数据库是否正常连接	控制中心是否与数据库正常连接		
安全事件是否正常保存	服务器硬盘空间是否充足	>5GB		
	是否生成昨天报表			
	是否生成当天实时报表			

（2）定期检查入侵检测系统的安全事件信息是否正常备份包括：

工作内容：每天生成昨天的安全事件统计报表以及当天的实时报表，将报表上报给安全管理人员。

工作频率：每天。

工作时间：1h。

工作角色：安全监控人员。

工作制度：每天做一次 24h 统计报表，对于发现的重点事件、重点 IP 应做分类报表及时上报给安全管理人员。

（3）安全事件分析包括：

工作内容：分析入侵检测系统检测结果，获得安全事件信息。

工作周期：每天。

工作时间：根据实际情况而定，1h 左右。

工作角色：安全管理人员。

需要记录表格：无。

安全事件分析详细工作：根据入侵检测系统检测的事件结果，以及根据现场的状况，由安全管理人员判断安全事件的分类级别，根据级别进行相应的上报和流程处理。

3）防病毒服务器管理

（1）防病毒服务器升级检查包括：

工作内容：

- ❑ 检查防病毒服务器病毒库下载是否正常，如果不正常及时联系厂商进行问题解决；
- ❑ 在防病毒系统每次升级后，记录每次版本变更版本号，定期记录病毒库的版本；
- ❑ 对重要的服务器，定期抽查防病毒客户端的病毒库升级情况。

工作频率：每天。

工作时间：1h。

工作角色：安全管理人员。

需要执行流程：一般安全事件处理流程。

防病毒服务器升级检查详细工作：

- ❑ 安全管理人员每天检查防病毒服务器的病毒库的自动升级情况，如果自动升级不成功，手动进行升级；
- ❑ 如果手动升级不成功或连续三次检查自动升级不成功，由安全管理人员根据“一般安全事件处理流程”进行解决，
- ❑ 安全管理人员在防病毒系统每次升级后，记录每次升级后版本的版本号，填写“防病毒服务器版本表”；
- ❑ 安全管理人员每天记录防病毒系统的病毒库的最新版本，填写“防病毒服务器版本表”。

（2）服务器防病毒客户端运行状况检查包括：

工作内容：定期抽查重要服务器防病毒客户端的运行情况，检查重点服务

器的病毒库版本是否为最新。

工作频率：每月。

工作时间：1h。

工作角色：系统管理人员。

需要记录表格：无。

需要执行流程：无。

服务器防病毒客户端运行状况检查详细工作：

- 由安全管理人员每周抽查重要服务器的防病毒客户端是否正常运行；
- 对于没有正在运行客户端的服务器，启动客户端防护服务；
- 对于客户端的病毒库版本和服务器不一致的情况，应对客户端的病毒库进行升级，与服务器的病毒库版本保持一致。

4）补丁管理

服务器及网络设备补丁安装工作包括：

工作内容：

- 执行重要服务器的补丁安装工作；
- 跟踪重要系统、服务器及网络设备的补丁安装版本和记录。

工作频率：无。

工作角色：安全管理人员。

需要执行流程：无。

重要服务器及网络设备补丁安装详细工作：

- 安全管理人员负责重要服务器和网络设备的补丁安装工作；
- 安全管理人员协调厂商完成重要服务器的安装工作，在安装前制定补丁安装计划，安装计划包括补丁安装背景描述、安装时间、安装各方人员、具体的实施方案、在安装过程对业务的影响、是否对业务造成中断、实施前备份内容、应急回退方案等内容；
- 各科室领导、安全管理人员及本次安装涉及技术人员对安装方案中每项内容进行审核，确认无误后开始安装工作；
- 安全管理人员根据补丁安装计划，在规定的时间执行由厂商完成补丁安装工作，安全管理人员监督整个安装过程是否按着计划进行；
- 在每次补丁安装完成后，记录补丁安装版本号和安装信息，填写“系统补丁安装记录表”。

5）账号与口令管理

（1）账号分类包括：

工作内容：将日常工作使用的账号根据作用和使用范围进行分类。

工作频率：无。

工作角色：安全管理人员。

需要记录表格：无。

需要执行流程：无。

账号分类详细工作：将各专业系统网络设备、服务器等操作系统账号、数据库账号统称为维护账号；将各应用系统账号及 OA 账号统称为办公账号。维

护账号包括超级权限用户和普通维护用户。办公账号权限管理由各应用系统进行保障，因此基础安全工作内容中主要是针对维护账号进行管理。

（2）账号创建及变更管理包括：

工作内容：当新员工来到公司、现有员工需要发生岗位和职责变化的情况下，根据“账号创建及变更流程”进行管理。

工作频率：无。

工作角色：安全管理人员。

需要执行流程：账号创建及变更流程。

账号创建及变更管理详细工作：

- 任何系统在建设实施过程中创建系统维护账号，该账号由系统管理人员和安全管理人员进行保存和维护。
- 当新员工来到公司、现有员工需要发生岗位和职责变化的情况下，室经理应该自动发出该员工需要的用户账号创建通知书、权限变更通知书。
- 室经理根据申请人的岗位职责进行审核，确认该员工的工作职责需要访问一个或多个受控系统，满足创建用户的条件。如果员工的工作职责不需要访问任何受控系统，则应拒绝申请。
- 如果部门内批准申请，则应将申请书转交至业务系统的所有者，由其室经理批准后，以书面或电子邮件的形式通知业务系统维护部门相关系统的系统管理员执行具体的创建用户操作。
- 符合条件并经室经理和部门经理审评后，由各系统安全管理人员创建用户，设置初始密码，将用户信息提交给申请人本人并签收，并应敦促申请人尽快更改初始口令。安全管理人员建立“系统账号表”，包括账号创建时间、账号申请人员等。当某用户需要超级权限时，应在其原有的用户 ID 之外，另行设置一个授予了超级权限的特殊账户（超级权限应是不同于一般商业用途的用户 ID 的另一个 ID）。

账号创建和变更流程如图 11-7 所示。

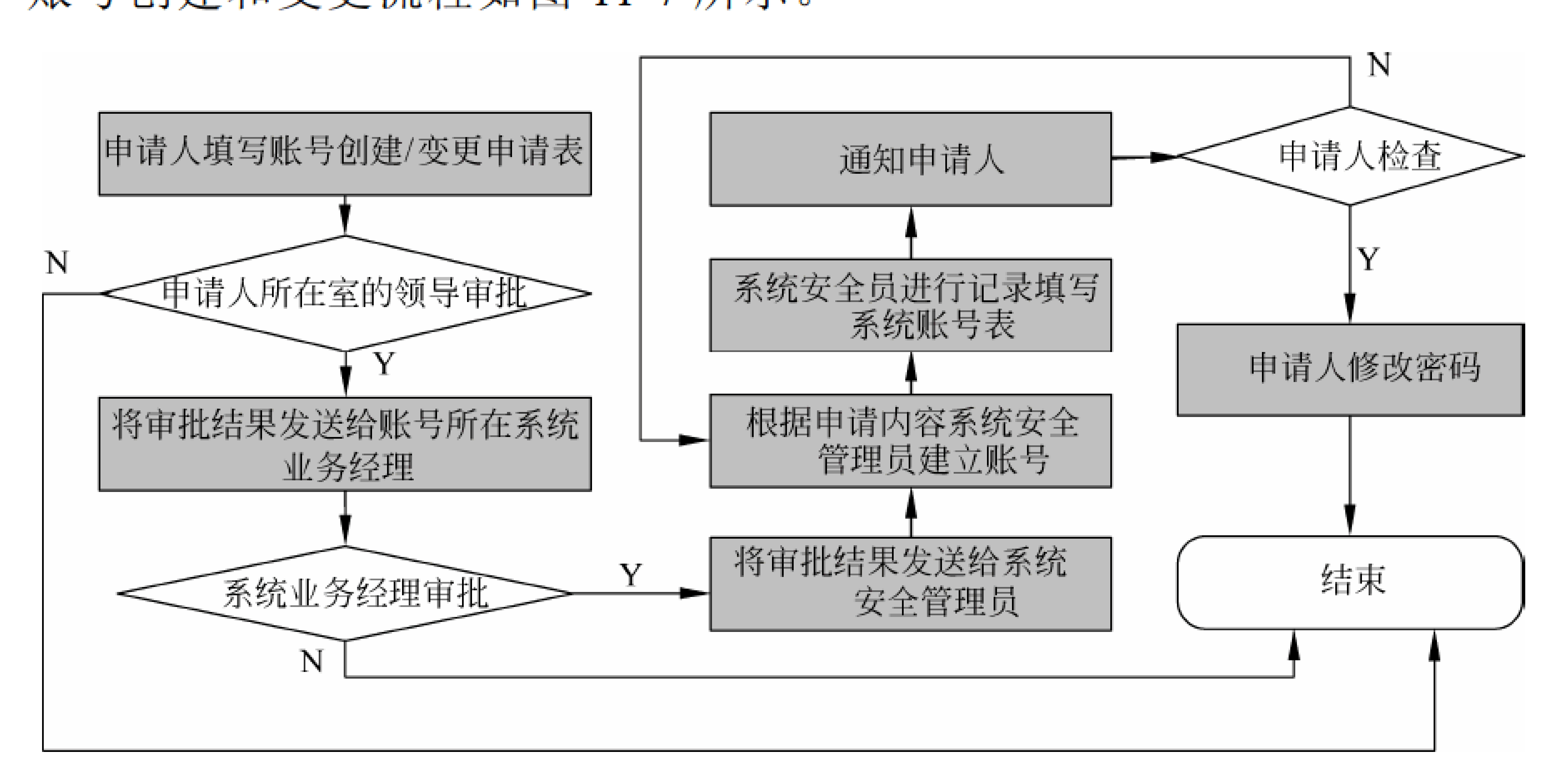


图 11-7　账号创建和变更流程

需要记录表格：账号创建和变更申请表（见表 11-3）。

- ❑ 本表格用于在每次账号申请和变更时填写，随需要而定，不具有周期性；
- ❑ 本表格不用于值班系统中。

表 11-3 账号创建和变更申请表

申请人		申请日期	
所属部门		工作岗位	
申请目的			
需要申请账号的业务系统			
账号名及需要权限描述			
员工部门经理意见及签字			
业务系统维护部门经理意见及签字			
系统管理员账号生成完毕签字			
账号接收完毕签字			

（3）第三方账号申请及变更管理包括：

工作内容：对第三方代维人员在维护系统过程中的账号进行集中管理。

工作频率：无。

工作角色：安全管理人员。

需要记录表格：无。

需要执行流程：第三方人员账号申请流程。

第三方账号申请及变更管理详细工作：

- ❑ 与第三方厂商签署保密协议；
- ❑ 对于第三方维护人员需要进行账号申请，必须由负责与第三方接口的人员向各室经理提出申请，填写第三方账号申请表，说明需要所具有的权限范围，说明使用时间；
- ❑ 由第三方接口人员将申请表发给室经理进行审批，其他流程如账号创建和变更流程的后续流程。

第三方账号创建和变更流程如图 11-8 所示。

（4）账号审计包括：

工作内容：对系统中的各种维护账号使用情况进行周期性审计，检查不合法和长久不用的账号。

工作频率：每季度。

工作时间：根据系统账号的数量决定工作时间，1 周左右。

工作角色：安全管理人员。

需要记录表格：无。

需要执行流程：无。

账号审计详细工作：

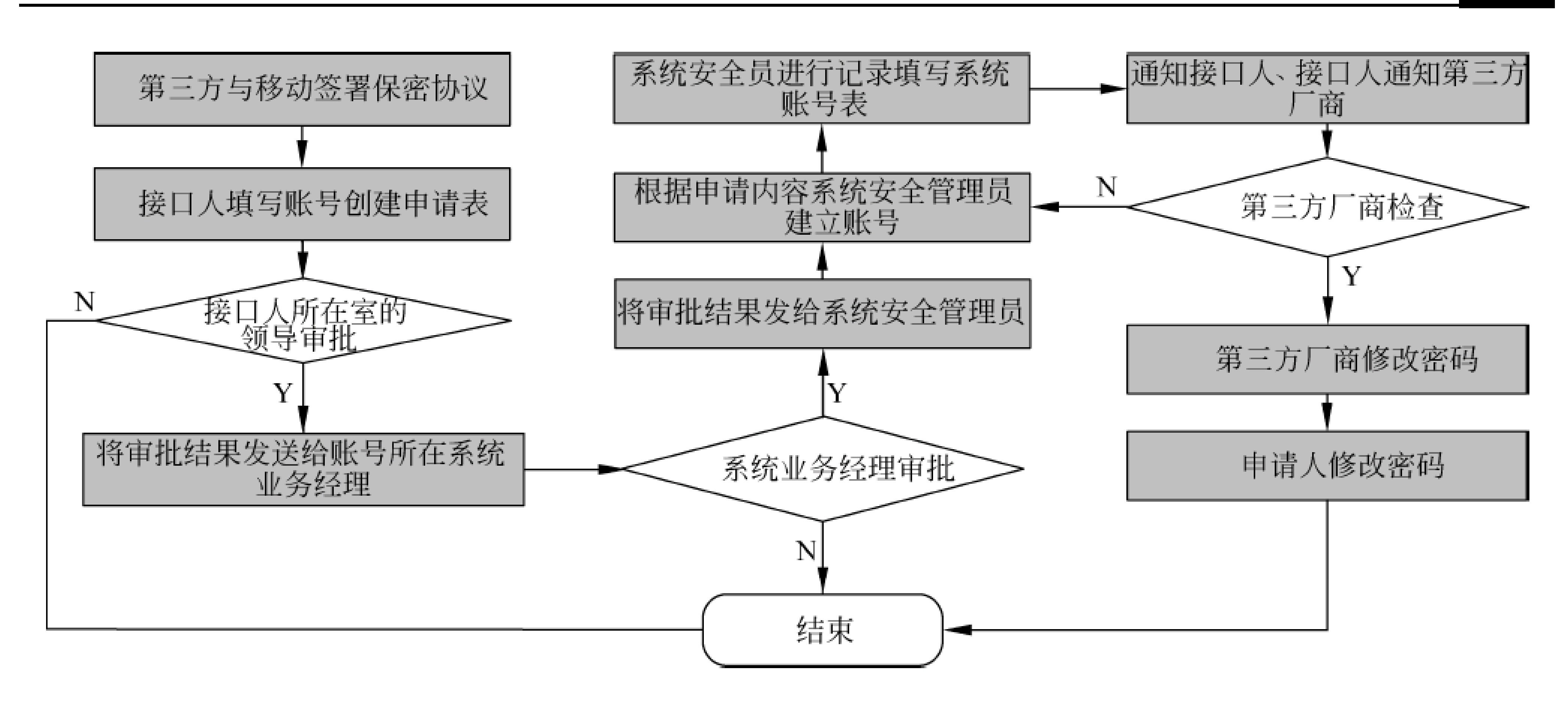


图 11-8　第三方账号创建和变更流程

- 安全管理人员每个季度对重要系统和服务器的维护账号进行人工审计。
- 人工审计内容包括系统目前账号名称、权限及对应的人员，并与系统账号表中的项目进行审计。
- 在审计过程中发现在系统账号表中未出现的账号，即认定是非法账号。
- 在审计过程中发现在系统账号表中显示某一账号的管理权限与实际不一致的账号，即认定是不合理账号。
- 对于第三方账号，检查该账号是否还在使用周期内，如果不在即认为是非法账号。
- 对于上述发现的非法和不合理账号，形成本次审计的结果信息。

（5）账号清理包括：

工作内容：根据账号审计的结果，对于不合法及长久不用的账号进行公示清理。

工作周期：每季度。

工作时间：根据系统账号的数量决定工作时间，1 周左右。

工作角色：安全管理人员。

需要记录表格：无。

需要执行流程：无。

账号清理详细工作：

- 对于审计结果进行公布，对于非法账号公示通知进行删除，对于不合理账号通知修改为正确权限。
- 如果在三个工作日内没有反馈意见，按公布的操作执行。
- 当账号的使用者离职时，在离职前将账号交接给该系统安全管理人员使用后 12h 内，由该系统管理人员修改密码，并变更系统账号表中的相应记录。

（6）第三方账号使用管理包括：

工作内容：对第三方维护的使用账号进行明确管理和约束。作为一项管理

制度，需要第三方人员在使用系统账号时遵守。

工作角色：安全管理人员。

需要记录表格：无。

需要执行流程：无。

第三方账号使用管理详细工作：

- ❑ 第三方人员拥有任何系统上的权限的前提是其所属的公司必须与第三方签署保密协议，保证其不滥用权限和账号。
- ❑ 第三方账号必须在申请的时间范围内使用，如果超过使用时间仍然需要使用该账号，由第三方接口人再提出变更需要，延长时间。
- ❑ 原则上，第三方人员不能使用超级用户的权限，如果有特殊需要可在安全管理人员的监督下使用超级账号，在第三方人员归还该账号 12h 内，系统管理人员必须修改超级用户密码。
- ❑ 分配给第三方公司人员的账号，应该保证每个人员拥有单独账号，而不混用。

（7）口令管理包括：

工作内容：加强口令管理，包括制定账号生成原则和维护原则。

工作频率：无。

工作角色：安全管理人员。

需要记录表格：无。

需要执行流程：无。

口令管理详细工作：

- ❑ 设置“口令生成原则”（见表 11-4），在账号使用者修改账号口令时遵守口令生成原则进行口令设置。
- ❑ 设置“口令维护周期和口令使用原则”，在账号维护周期内进行口令修改。

表 11-4　口令生成原则及口令维护原则

口令生成原则：
口令必须具有足够的长度和复杂度，使口令难以被猜测
口令在一定时间或次数内不能循环使用
不同账号的口令应当不同，并且没有直接联系，以保证不可由一个账号的口令推知其他账号的口令
同一账号前后两个口令之间的相同部分应当尽量减少，降低由前一个口令分析出后一个口令的机会
口令不应当取过于简单的字符串，如电话号码、使用者的姓名、宠物、生日或其倒序，6 位字符都相同、6 位连续字符等易于猜测的信息
开户时设定的初始口令必须是随机产生的口令，而不能是相同或者有规律的口令
用户所使用的任何具备系统超级用户权限（包括并不限于系统管理员账号和有 sodu 权限账号）账号口令必需和这个用户其他账号的口令均不相同

续表

当使用 SNMP 时，communication string 不允许使用默认的 Public、Private 和 System 等，并且该 communication string 不应该和系统的其他口令相同，应该尽量使用 SNMPv2 以上的版本
口令维护原则：
不要把自己的口令共享给他人
不要在 E-mail 中写口令
在别人面前谈论的时候，不要提到口令
不要暗示自己口令的格式
不要在调查中给出口令
不要告诉家人口令
休假时不要把自己的口令告诉他人
不要使用非公司授权和许可的口令记忆软件
口令不应该记在非经特别保护的纸面上，不能未经加密存储在电子介质中
所有系统管理员级别的口令（如 root、enable、NT administrator、DBA 等）在没有使用增强口令的情况下，必需以较短周期进行密码更改（口令周期见口令周期管理）
以下情况时，相关口令必须立即更改（12h 内）：
掌握口令的网络管理人员离开岗位
工程施工、厂商维护完成
因工作需要，由相关厂家或第三方公司使用了登录账号及密码后
一旦有迹象表明口令可能被泄露

6）周期性安全审计

（1）系统漏洞检查包括：

工作内容：定期利用漏洞扫描工具对各指定的服务器和终端进行扫描。扫描内容包括弱口令、系统漏洞、开放的端口和服务等，对每次扫描结果进行存档，并统计和跟踪漏洞的变化情况。

工作频率：每季度。

工作时间：根据被扫描系统的范围以及承载业务的重要性决定扫描的时间，1 周左右。

工作角色：安全管理人员。

需要执行流程：无。

系统漏洞检查详细工作：

- 扫描可采用系统中已有的漏洞扫描产品，也可以由指定的安全顾问公司完成。
- 扫描前由系统安全管理人员制定扫描计划，包括扫描时间、各方人员安排、具体扫描方案、扫描过程中应急回退方案等内容。
- 各科室领导、安全管理人员及本次扫描过程中涉及的技术人员对安装方案中每项内容进行审核，确认无误后开始扫描工作。

- 对扫描过程和结果进行记录，包括扫描报告、扫描时间、扫描范围、漏洞统计（主要统计类型分为弱口令、系统漏洞、开放端口）、风险级别统计等，扫描记录用当时时间命名。
- 比较本次扫描结果与最近一次扫描结果，统计增加漏洞的数量、各种风险级别的变化情况等，用以反映本季度安全工作的成果。
- 纳入扫描范围的业务系统的相应科室安全负责人跟进整个安全扫描，如果在扫描中发现新的安全漏洞，就要求厂家进行系统升级或进行漏洞补丁加载。如果安全漏洞无法通过补丁加载消除，则需要与数业室、厂家及安全顾问公司共同协商，用其他方法解决，比如关闭主机或防火墙端口等方式，尽量杜绝因系统安全漏洞原因引起的安全问题。

周期性扫描记录表现如表 11-5 所示。

表 11-5 周期性扫描记录表

周期性扫描记录表			
扫描时间	扫描系统	扫描设备名称列表	扫描漏洞总数
高风险漏洞数量	中风险漏洞数量	低风险漏洞数量	弱口令造成漏洞数量
系统漏洞数量	开放端口造成漏洞数量	本次新增漏洞数量	扫描执行人

（2）文档检查包括：

工作内容：每季度对各科室管辖系统在基础安全工作中所形成的安全文档进行检查。

工作频率：每季度。

工作时间：根据被检查文档的范围和数量决定文档检查工作的时长，1 周左右

工作角色：安全管理人员。

需要记录表格：周期性扫描记录。

需要执行流程：无。

文档检查详细工作：

- 每季度由各科室的系统管理员组成的检查小组，对各科室管辖系统在基础安全工作中所形成的安全文档进行检查，检查的文档包括防火墙日常安全检查表、IDS 日常安全检查表、防病毒服务器版本表、系统补丁安装记录表、账号申请表、系统账号表、扫描记录等。
- 对于如防火墙日常安全检查表需每天填写的表格，一个季度内如果缺少记录或记录不完整达 5 次则认为安全日常工作为不合格。
- 检查每个系统是否有“防病毒服务器版本表、系统补丁安装记录表、账号申请表、系统账号表、扫描记录”信息。

- 对检查结果进行公示。

7）新入网系统安全检查

（1）系统漏洞审计包括：

工作内容：在每个新业务系统验收入网之前，应对此系统进行一次全面的安全扫描及必要安全补丁加载。

工作频率：无。

工作角色：安全管理人员。

需要记录表格：无。

需要执行流程：无。

系统漏洞审计详细工作：

- 对新接入的系统利用漏洞扫描工具对各指定的服务器和终端进行扫描。扫描内容包括弱口令、系统漏洞、开放的端口和服务等。对扫描结果由厂商进行加固和修补，在没有高风险的漏洞情况下系统方能接入网络。
- 由新接入系统的负责人提出漏洞扫描申请，扫描时可利用系统现有的扫描工具也可由顾问公司完成。
- 扫描前由新接入系统的负责人制定扫描计划，包括扫描时间、各方人员安排、具体扫描方案等内容。
- 扫描方案经厂商确认后，执行扫描工作，将扫描结果发给厂商。
- 如果扫描结果显示，新接入的系统存在高风险的漏洞，则不允许系统接入网络。
- 对发现的高风险的漏洞由厂家进行加固和修补处理后，再进行同样扫描后不出现这样问题才可接入系统。

（2）提交系统安全相关文档包括：

工作内容：在新系统接入时，厂商需提交和安全相关的文档。

工作频率：无。

工作角色：安全管理人员。

需要记录表格：无。

需要执行流程：无。

提交系统安全相关文档详细工作：

- 在新系统接入时，厂商需提交和安全相关的文档，由系统安全管理人员进行保管。
- 文档内容包括系统正常运行需开放的端口、系统正常运行时需要对防火墙策略调整的内容、服务器已经安装的补丁列表、系统软件版本列表等信息。

8）安全事件管理

（1）安全事件等级管理包括：

工作内容：定义影响网络安全的各种事件的等级，根据安全事件的破坏性

及安全事件发生的资产价值，对安全事件进行分类。

工作频率：无。

需要记录表格：无。

需要执行流程：无。

安全事件详细工作：安全事件分为重大安全事件、严重安全事件、一般安全事件和安全预警信息。

- 重大安全事件：由于 DDoS 攻击造成的业务系统和网络不能对外提供服务；业务网络中爆发大规模蠕虫病毒，造成网络瘫痪；业务支撑系统、生产系统的服务器被黑客攻击造成无法提供正常服务；业务支撑系统、生产系统感染病毒，无法提供正常服务。
- 严重安全事件：黑客对非生产系统进行攻击，造成其无法提供正常服务；非生产系统的 Win 平台服务器感染病毒，无法提供正常服务；防火墙发生故障，不能进行正常工作。
- 一般安全事件：各种终端感染病毒，无法正常工作；入侵检测、防病毒服务器、补丁管理服务器等安全产品发生故障，不能进行正常工作。
- 安全预警信息：发布可能发生的安全事件信息，提醒安全管理人员注意。

（2）安全事件处理流程包括：

工作内容：根据事件的安全级别执行相应的处理流程。本项工作不用于值班系统管理。

工作周期：无。

执行人员：安全管理人员、安全监控人员、系统管理人员以及各级领导等。

需要记录表格：无。

需要执行流程：安全事件处理流程。

安全事件处理流程详细工作：

- 对于重大安全事件按重大安全事件处理流程进行解决。出现重大安全事件，必须在 30min 内上报省公司安全领导小组，迅速组织厂商、安全顾问公司人员现场抢修。
- 对于严重安全事件按严重安全事件处理流程进行解决。出现严重安全事件，必须在 24h 内解决。在 60min 内上报省公司上级单位或部门，迅速组织厂商、安全顾问公司人员现场抢修。
- 对于一般安全事件按一般安全事件处理流程进行解决。出现一般安全事件，必须在 48h 内解决。若在规定时限内不能解决安全事件，则安全事件类型上升为严重安全事件。
- 对于预警信息按预警信息处理流程进行解决。

安全事件处理流程如图 11-9 所示。

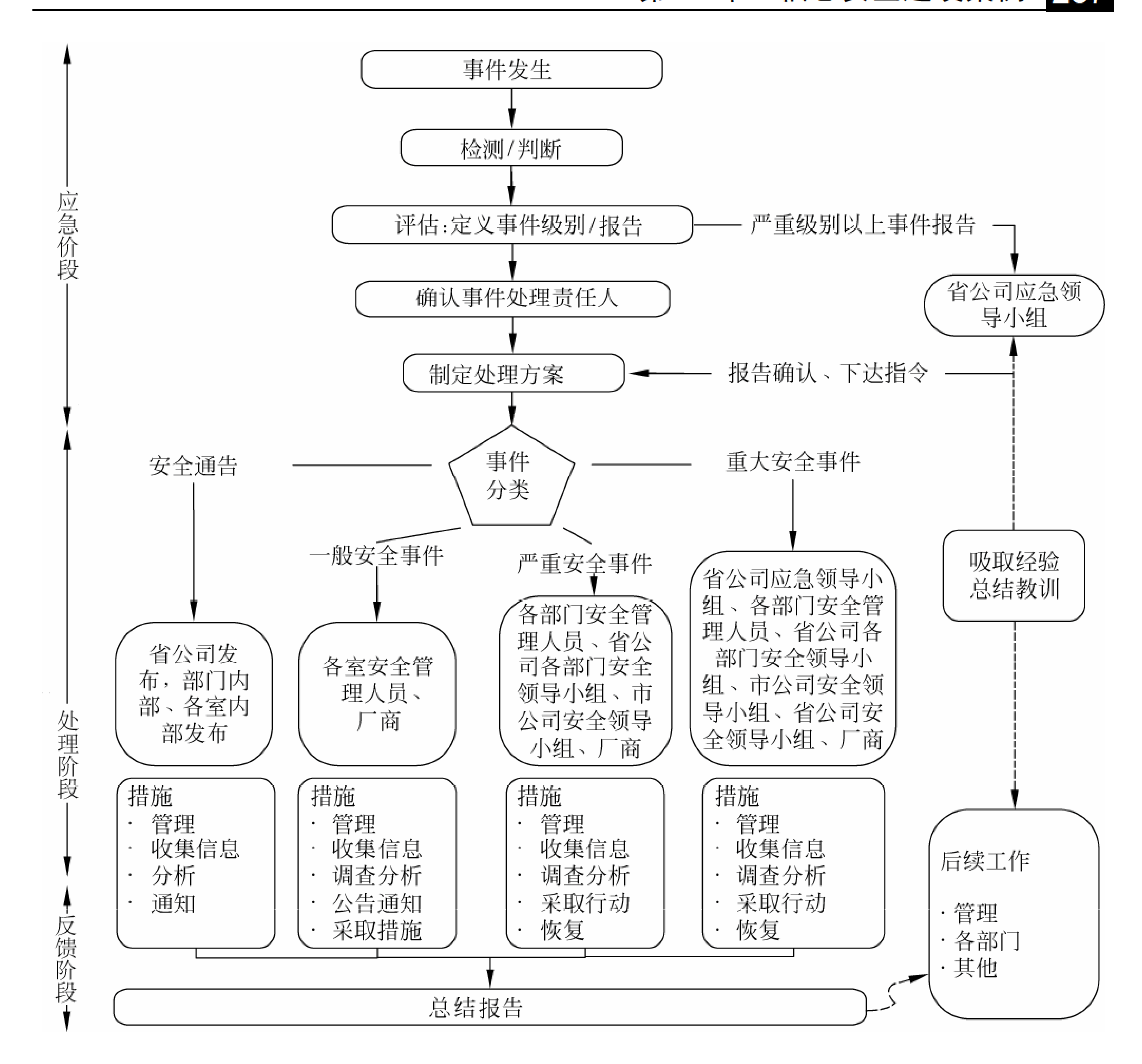


图 11-9　安全事件处理流程图

（3）安全事件上报和统计包括：

工作内容：对于安全事件上报以及进行安全事件的统计管理。本项工作不用于值班系统管理。

工作频率：无。

工作角色：安全管理人员、安全监控人员、系统管理人员。

需要记录表格：无。

需要执行流程：无。

安全事件上报和统计详细工作：

- 当发生重大安全事件时，各级安全维护人员应立即逐级上报，直至省公司安全管理小组，不得延误。重大安全事件自障碍确认至上报到省公司安全管理小组不得超过 30min，严重安全事件上报时间不能超过 60min。必要时可越级上报。
- 重大安全事件处理完毕，恢复生产后，各省公司安全管理小组（由各系

统安全管理人员执行整理工作）应就安全事件现象、影响范围和时间、安全事件原因、解决处理情况等整理形成正式的文档说明进行备案，建立安全事件处理知识库。

- 安全事件处理知识库可以使用现有故障处理知识库进行管理。

（4）工单与安全公告处理包括：

工作内容：处理省公司发布的涉及安全的工单。

工作频率：无。

工作角色：安全管理人员、安全监控人员、系统管理人员。

需要记录表格：无。

需要执行流程：无。

工单与安全公告处理详细工作：

- 由于目前工单处理系统并不区分故障工单和安全事件工单，因此各系统安全管理人员根据现有的工单处理流程，处理与安全有关的工单。
- 安全管理人员接收省公司和安全部门发布的安全通告，将通告转发给各科室内部、各系统内部人员。

11.4 信息安全技术建设案例

11.4.1 项目背景

《电业局二次系统安全防护方案》是按照国家电监会第5号令（电力二次系统安全防护规定）及《全国电力二次系统安全防护总体方案（第8稿）》的要求，并结合电业局的二次系统现状，按照某省电力公司统一安排的二次系统安全防护总体方案实施步骤，对电业局的二次系统进行全面的逻辑边界分析清理，以此为依据进行二次系统的安全分区，结构调整。

11.4.2 项目目标

二次系统安全防护是电力系统安全生产的重要组成部分，重点是抵御黑客、病毒、恶意代码等通过各种形式对系统发起的恶意破坏和攻击，尤其是集团式攻击，重点保护实时闭环监控系统及调度数据网络的安全，防止由此引起的一次系统事故或大面积停电事故，以及二次系统的崩溃或瘫痪。

1. 安全防护目标

（1）防止通过外部边界发起的攻击和侵入，尤其是防止由攻击导致的一次系统的事故以及二次系统的崩溃。

（2）防止内部未授权用户访问系统或非法获取信息和侵入以及重大的非法操作。

2．电力二次系统的安全防护策略

（1）安全分区。根据系统中业务的重要性和对一次系统的影响程度进行分区，所有系统都必须只置于相应的安全区内，对实时控制系统等关键业务采用认证、加密等技术实施重点保护。

（2）网络专用。建立调度专用数据网络，实现与其他数据网络的物理隔离，并以技术手段在调度数据网络上形成相互逻辑隔离的实时子网和非实时子网，以保证上下级各安全区的纵向互连仅在相同安全区进行，避免安全区纵向交叉连接。

（3）横向隔离。采用不同强度的安全隔离设备使各安全区内的业务系统得到有效保护，关键是将实时监控系统与办公自动化系统等实行有效的安全隔离。隔离强度应达到或接近物理隔离。

（4）纵向认证。采用认证、加密、访问控制等手段实现数据的远方安全传输以及纵向边界的安全防护。

11.4.3　项目工作内容

1．安全分区划分

1）安全分区

根据电力二次系统的特点，各相关业务系统的重要程度和数据流程，整个电力二次系统划分为生产控制大区和管理信息大区，如图 11-10 所示。

生产控制大区采用电力调度数据网（SPDnet），管理信息大区采用电力企业数据网络及外部公共信息网。

生产控制大区可以分为控制区（安全区 I）和非控制区（安全区 II）；管理信息大区在不影响生产控制大区安全的前提下，根据各企业不同安全要求划分，一般可以划分为生产管理区（安全区 III）和管理信息区（安全区 IV）。

电力二次系统划分为不同的安全工作区，反映了各区中业务系统重要性的差别。不同的安全区确定了不同的安全防护要求，从而决定了不同的安全等级和防护水平。

根据电力二次系统的特点、目前状况和安全要求，整个二次系统分为四个安全工作区，即实时控制区、非控制生产区、生产管理区、管理信息区。

（1）安全区 I 是实时控制区，安全保护的重点与核心。凡是实时监控系统或具有实时监控功能的系统其监控功能部分均应属于安全区 I。

例如，调度自动化系统（SCADA/EMS）、集控操作主站系统和变电站自动化系统等，其面向的使用者为调度员、集控操作员和运行操作人员，数据实时性为秒级，外部边界的通信均经由电力调度数据网（SPDnet）的实时虚拟专用

网（VPN）。区中还包括采用专用通道的控制系统，如继电保护、安全自动控制系统、低频/低压自动减载系统、负荷控制系统等，这类系统对数据通信的实时性要求为毫秒级或秒级，是电力二次系统中最为重要的系统，安全等级最高。

（2）安全区 II 是非控制生产区。原则上不具备控制功能的生产业务和批发交易业务系统或系统中不进行控制的部分均属于安全区 II。

属于安全区 II 的典型系统包括电能量计量系统、发电侧电力市场交易系统等，其面向的使用者为运行方式、运行计划工作人员及发电侧电力市场交易员等，数据的实时性是分级、小时级。该区的外部通信边界为 SPDnet 的非实时 VPN。

（3）安全区 III 是生产管理区。该区包括进行生产管理的系统，典型的系统为雷电监测系统、气象信息接入等。本安全区内的生产系统采取安全防护措施后可以提供 Web 服务。该区的外部通信边界为电力数据通信网（SPTnet）。

（4）安全区 IV 是管理信息区。该区包括办公管理信息系统、客户服务等。该区的外部通信边界为 SPTnet 及因特网。该区在本文件中不作详细规定，但必须具备必要的安全防护措施。

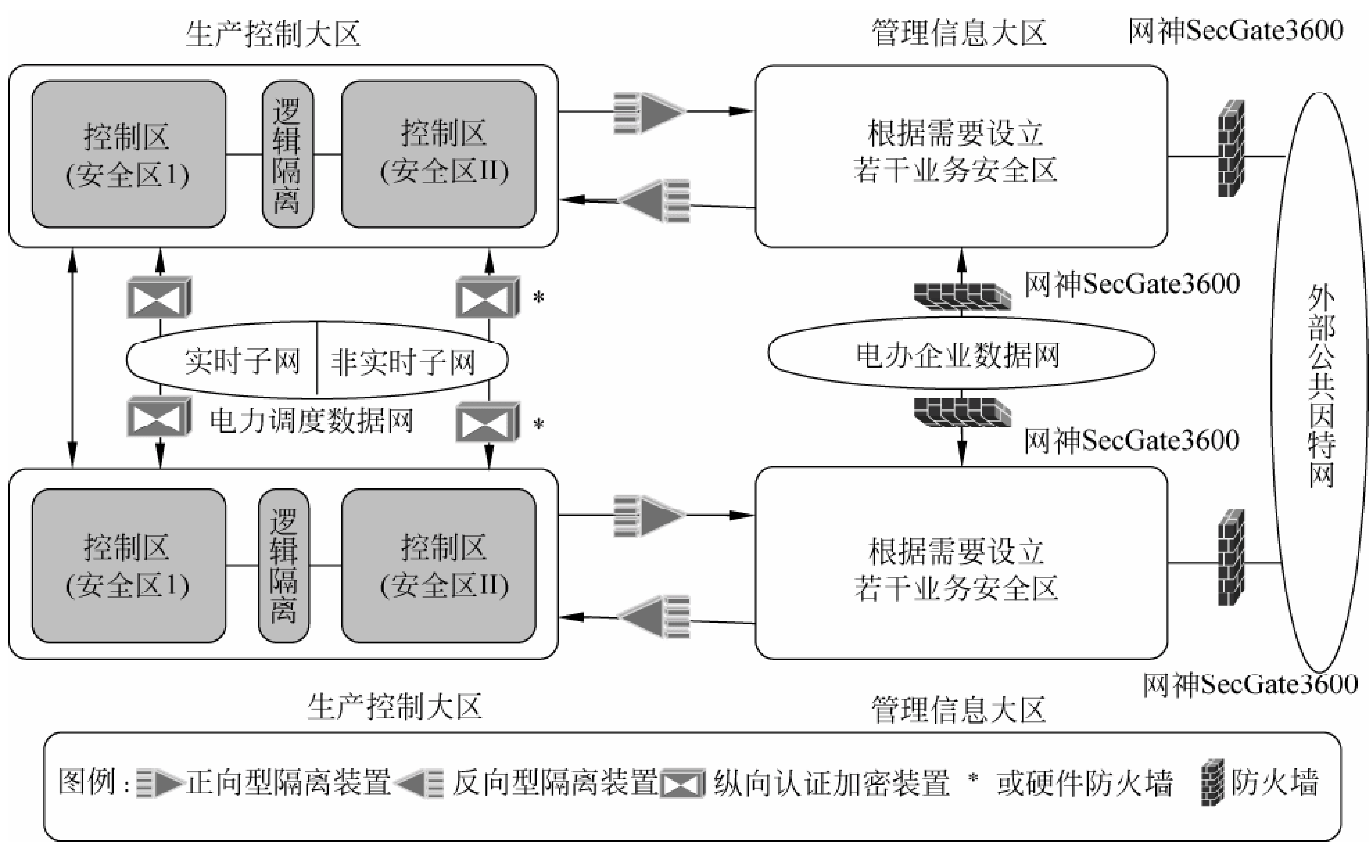


图 11-10 安全分区的划分

2）安全区间的隔离装置的基本要求

在各安全区之间均需选择适当安全强度的隔离装置。具体隔离装置的选择不仅需要考虑网络安全的要求，还需要考虑带宽及实时性的要求。隔离装置必须是国产设备并经过国家或电力系统有关部门认证。

（1）生产控制大区不得与管理信息大区直接联系，它们之间必须采用经有关部门认定核准的电力专用安全隔离装置。专用安全隔离装置应该达到或接近物理隔离的强度。严格禁止 E-mail、Web、Telnet、Rlogin 等网络服务和以 B/S

或 C/S 方式的数据库访问功能穿越专用安全隔离装置，仅允许纯数据的单向安全传输。专用安全隔离装置分为正向型和反向型。从生产控制大区往管理信息大区必须采用正向安全隔离装置单向传输信息；由管理信息大区往生产控制大区的少量单向数据传输必须经反向安全隔离装置。反向隔离装置采取签名认证和数据过滤措施，仅允许纯文本数据通过，并严格进行病毒、木马等恶意代码的查杀。

（2）安全区 I 与安全区 II 之间必须采用经有关部门认定核准的硬件防火墙或相当设备进行逻辑隔离，应禁止 E-mail、Web、Telnet、Rlogin 等服务穿越安全区之间的隔离设备。

（3）安全区 III 与安全区 IV 之间应采用经有关部门认定核准的硬件防火墙或相当设备进行逻辑隔离。

3）各安全区内部安全防护的基本要求

对生产控制大区的要求：

（1）禁止生产控制大区内部的 E-mail 服务，禁止安全区 I 的 Web 服务。

（2）允许安全区 II 内部 B/S 结构的系统，系统必须采取措施进行封闭。允许安全区 II 纵向安全 Web 服务，经过安全加固且支持 HTTPS 的安全 Web 服务器和 Web 浏览工作站应在专用网段，Web 浏览工作站与 II 区业务系统工作站不得共用，而且必须由业务系统向 Web 服务器单向主动传送数据。

（3）生产控制大区内的重要业务（如 SCADA、电力交易）应该逐步采用认证加密机制。

（4）生产控制大区内的业务系统间应采取访问控制等安全措施。

（5）生产控制大区内的拨号访问服务，用户端应该使用 UNIX 或 Linux 操作系统，且采取认证、加密、访问控制等安全防护措施。

（6）生产控制大区边界上可考虑部署入侵检测系统 IDS。

（7）生产控制大区可考虑部署安全审计措施，应将安全区安全管理系统、IDS 管理系统、敏感业务服务器登录认证和授权、应用访问权限相结合。

（8）生产控制大区应采取防恶意代码措施。病毒库和木马库的更新应该离线进行，不得直接从因特网下载。

（9）安全区 I/II 内的系统必须经过安全评估。

对管理信息大区的要求：

（1）安全区 III 允许开通 E-mail、Web 服务。

（2）安全区 III 的拨号访问服务必须采取访问控制等安全防护措施。

（3）安全区 III 的系统应该部署安全审计措施，如 IDS 等。

（4）安全区 III 的系统必须采取防恶意代码措施。

2．企业电业局二次系统安全防护方案

根据二次系统安全防护总体框架的要求，企业电业局二次系统安全防护的基本技术措施为“安全分区、网络专用、横向隔离、纵向认证”。

1）规划网络结构

整个网络结构分为四个区，各区之间有明确的分界线，如图 11-11 所示。以下按照安全分区及应用系统详细介绍网络改造及网络安全产品部署建议。

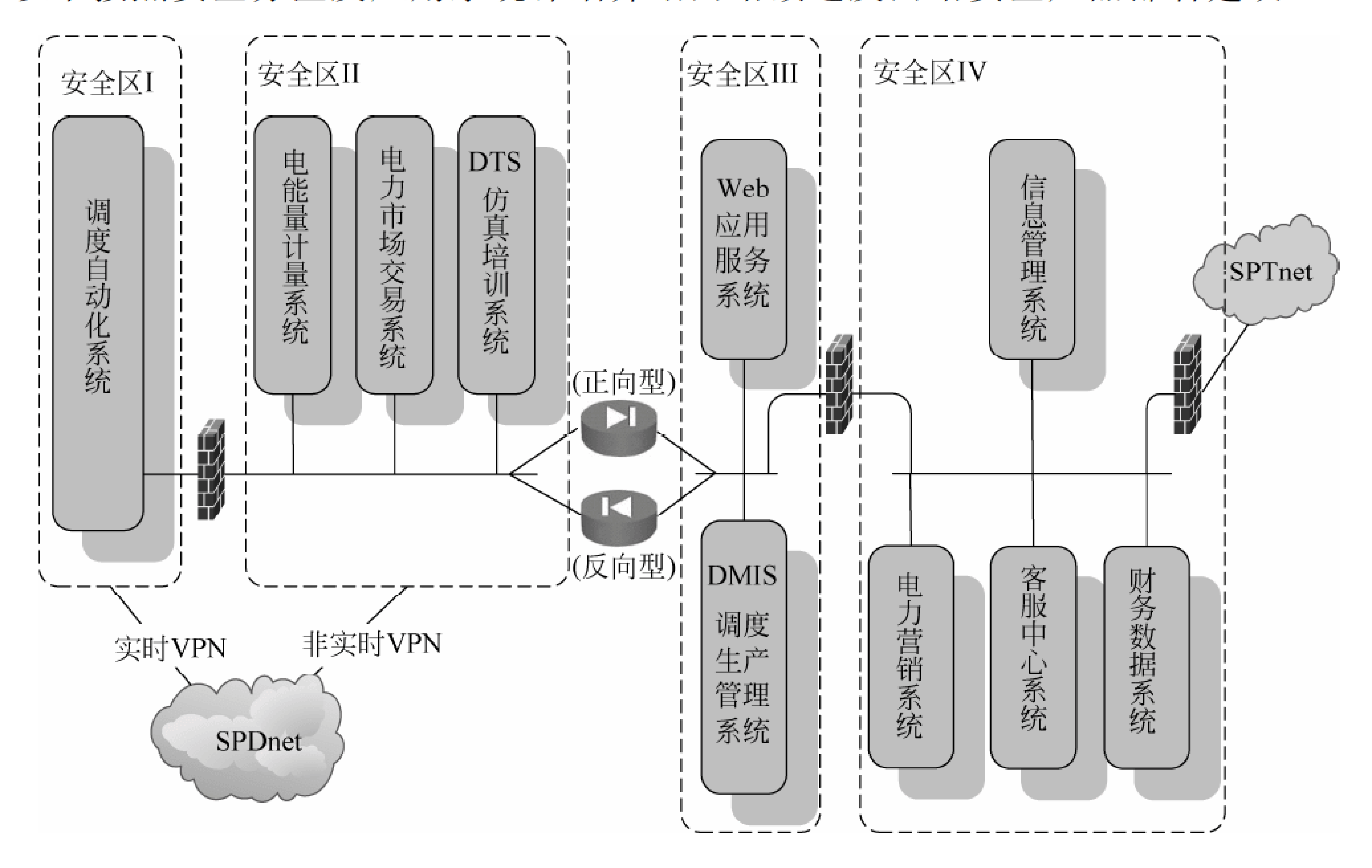


图 11-11　整个网络区域的规划

2）安全区 I、II 业务系统安全产品部署

调度自动化系统与分控中心属安全区 I 业务系统，采用光纤线路直接连接，可看作调度自动化局域网的延伸，安全性可以得到保证，故不再在调度自动化与分控中心之间部署网络安全产品。与省调采用专用通道连接，与厂站采用专用通道 RTU 连接，今后可采用线路加密方式，目前暂不考虑。

安全区 I 网络结构改造及安全防护产品部署如下：

（1）将 Web 服务器外移至 III 区（因现有 EMS 系统 Web 服务器无独立数据　库，故需新增服务器并建独立数据库，与 I 区内服务器同步）；横向增加对内网关一台，并增加具备逻辑隔离功能的接入交换机和硬件防火墙与安全区域 II 进行隔离。

（2）通过拨号服务器（RAS）接入 EMS 系统的 LAN，在 RAS 和 LAN 之间必须增加拨号认证加密装置，拨入端配相应的数字证书（证书由电力调度机构签发）。

（3）在安全区 I 的横向和纵向交换机上增加一套双探头的入侵检测探头，同时监测横向和纵向交换机，区内不再做部署。

（4）其他 SCADA/EMS 系统包括通过调度数据网与省调连接的省调 EMS 系统和现有的两个集控操作主站系统。

3）安全区 IV 各应用业务系统网络安全产品部署

安全区Ⅳ包括电业局各应用服务业务系统，如电力营销系统、客户服务系统、财务 FMIS 系统、办公自动化及 EIP 系统等。各应用业务系统均允许开通 Web 和 E-mail 等通用服务，但其数据均应通过横向防火墙隔离；可以提供拨号接入服务，但必须对拨号接入进行访问控制。

各应用系统之间应部署防火墙产品，在电业局到省公司的出口已有一台硬件防火墙；按照本方案对安全区 III、IV 的部署，只考虑安全区 IV 各个应用系统之间的防火墙产品部署。

考虑到本区内有些系统（如 EIP 系统、短信平台、电网经济运行分析软件等）会需要安全区 I、II 的生产数据，安全区 I、II 的数据都通过 Web 方式发布在安全区 III，所以在安全区 III、IV 之间必须考虑部署一台硬件防火墙。

4）安全区 III、IV 安全防护产品部署

计划增加配置以下设备：

（1）安全区 III 区增加具备逻辑隔离功能的接入交换机。

（2）安全 III 区与 IV 区之间必须增加经有关部门认定核准的硬件防火墙，作为安全逻辑隔离。

（3）安全区 IV 区与外网之间应有经有关部门认定核准的硬件防火墙，作为安全逻辑隔离（目前已有可暂不考虑）；在安全区 III/IV 的交换机上增加入侵检测系统 IDS（配置为双探头）。

安全区 III 与安全区 IV 网络安全产品部署如图 11-12 所示。

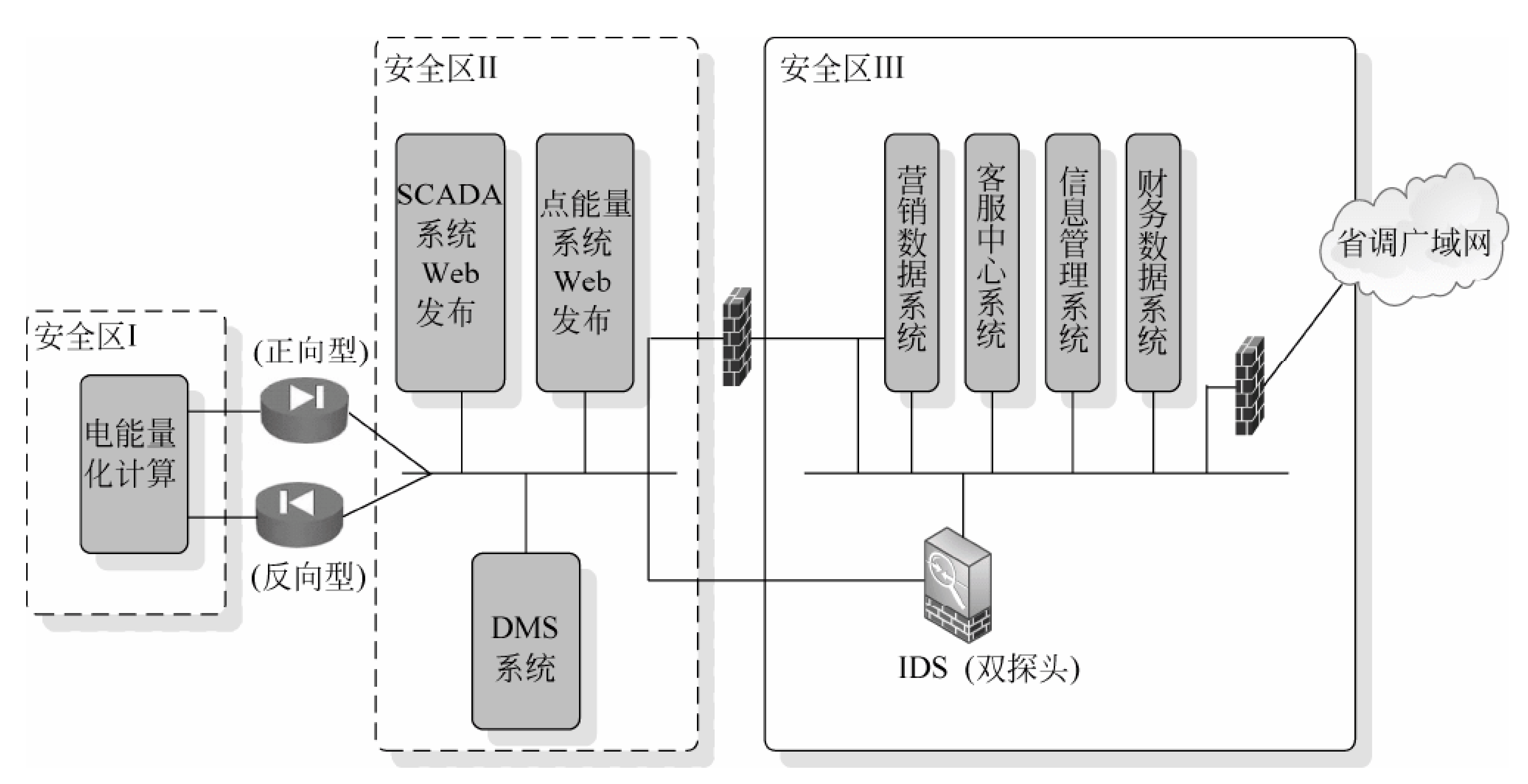


图 11-12　安全区域 III/IV 安全产品部署示意图

5）网络防病毒设计

对防病毒软件的要求和目标：

（1）病毒查杀能力强。

（2）厂商提供的杀病毒软件不仅要能保护文件，同时也要对各种服务器、

PC、网关等所有计算机设备进行保护，而且能从邮件、FTP 文件、网页、软盘、光盘等所有可能带来病毒的信息源进行监控和病毒拦截。

（3）要求具有一定程度的未知病毒识别能力，一旦防病毒软件发现一个文件可能携带病毒，它应该有能力提供一种解决方法对文件进行处理，以免系统或者文件受到未知病毒的破坏。

（4）对新病毒的反应能力强，可从软件供应商的病毒信息搜集网络、病毒代码的更新周期和供应商对用户发现的新病毒的反应周期三个方面体现。

（5）提供强大的病毒实时监测能力，并尽可能少地占用系统资源。

（6）提供快速、方便、灵活和简便的升级手段。

（7）应能智能安装、远程识别、管理方便、易于操作，统计和报表功能强大。

（8）提供多种报警手段，能通过电子邮件、打印机、寻呼机、手机或网络消息，传送各种病毒告警给携带病毒用户和系统管理员，并能提供标准输出，供其他系统对其告警信息二次开发。

网络防病毒系统应由以下四部分组成：

（1）在安全区 I 和安全区 III 建立中心级防病毒管理中心：可以管理到本安全区网络中的任何一台计算机，对区中的所有计算机统一进行病毒定义码的更新、防病毒政策的设定、病毒情况的监控，手动的、定时的病毒扫描及清除，病毒日志及汇总报表以及集中隔离未知病毒，并能隔离有病毒的客户端。

（2）网关级病毒防护：主要针对通过 Internet 出口连接点集中进行病毒扫描，对邮件的附件进行病毒过滤。

（3）群件服务器病毒防护：针对 Lotus Notes Domino 服务器这种协同工作机制的服务器进行病毒防护。

（4）客户端防病毒防护：针对各种桌面操作系统，进行病毒扫描和清除。

按照国调中心四安全区的划分，企业电业局的网络防病毒系统应该具备两套，以专用隔离装置为界，分别实施。对于安全区 III 的网络防病毒系统可以通过自动升级病毒库的方式进行在线升级，安全区 I/II 的病毒库只有通过网络安全专责定期进行手动升级病毒库。

6）网络安全评估与漏洞扫描

网络安全评估与漏洞扫描可发现网络和主机系统的安全漏洞，并提供安全解决建议，且对全网进行安全配置检查。

漏洞扫描能够扫描网络范围内的所有基于 TCP/IP 协议的设备，扫描的对象包括常见的操作系统、数据库、网络设备和应用系统等。能够对扫描对象的安全脆弱性进行全面检查，检查内容包括缺少的安全补丁、词典中可猜测的口令、不适当的用户权限、不正确的系统登录权限、操作系统内部是否有黑客程序驻留、不安全的服务配置等等。扫描信息全面完备，包括主机信息、账号信息、服务信息、漏洞信息等内容。具有强大的漏洞库和丰富的漏洞检查列表，漏洞库涵盖当前系统常见的漏洞和攻击特征，包括至少 30 个大类 1000 个以上漏洞特征描述。

漏洞扫描具有多线程扫描功能及断点扫描功能；提供多种扫描方式，在授权范围内进行单机扫描、分组扫描和全部扫描。要求可以从不同的网络位置对网络设备进行扫描；提供多种默认的扫描策略，并可按照特定的需求，针对不同的目标对象或目标群组，可以同时应用不同扫描策略。允许自定义扫描策略和扫描参数，实现不同内容、不同级别、不同程度、不同层次扫描；提供全自动定时扫描或多种计划扫描任务功能，按照用户指定的时间对指定的对象自动扫描，并自动生成报告；扫描的结果可生成详细的安全评估报告，报告具有易懂的漏洞扫描和详尽的修补方案建议，并提供相关的技术站点。提供灵活的报告格式，用户可以定制，根据管理层、技术主管和管理员不同需求产生灵活的报告格式；要求提供中文管理界面和生成中文报表，提供全面的在线帮助；可以根据任务要求灵活移动扫描位置，便于检查任务时携带、维护；能够定期进行漏洞升级，支持远程在线升级方式，自动完成升级过程。可以显示正在扫描任务详细信息的功能，显示等待扫描任务详细信息，对产品自身的参数进行配置；能够与主流入侵检测系统联动，实现对事件攻击效果的进一步验证；能够进行权限管理，对用户分级，提供不同的操作权限；对网络和主机进行漏洞扫描时，不对网络做任何修改，不造成任何危害。

网络安全评估漏洞扫描的要求如下：

（1）获得国家有关部门的认证。产品要求取得中华人民共和国公安部的《计算机信息系统安全专用产品销售许可证》、中国国家信息安全产品测评认证中心的《国家信息安全认证产品型号证书》、中国国家保密局测评中心颁发的《涉密信息系统产品检测证书》。

（2）采用国产化设备，具备自主知识产权。

（3）产品要求功能模块配置灵活，具有良好的可扩展性。

（4）安全产品要求界面友好，易于安装、配置和管理，并有详尽的技术文档。所有的图形界面与文档资料要求均为中文。

（5）要求厂家拥有稳定的服务保障和技术支持队伍，保证实施的服务质量和快速的服务响应时间。

7）改造后企业电网二次系统结构图

改造后企业电网二次系统结构如图 11-13 所示。

3. 系统安全防护对设备的要求

1）防火墙

为了实现 I/II 区、III/IV 区之间的横向逻辑隔离，需要部署防火墙系统。防火墙系统的主要技术要求如下：

（1）强大的应用级的防护能力。调度系统对外发布三公信息的 Web 服务器，极易受到黑客工具的扫描。黑客工具一般使用 HEAD 命令对 Web 服务器进行扫描，以防止在 Web 服务器上留下日志。防火墙可以通过设置安全策略阻断 HEAD 等命令并发出报警，替换服务器信息，防止外部攻击者获得有关服务器

的信息，保护内网服务器的安全。

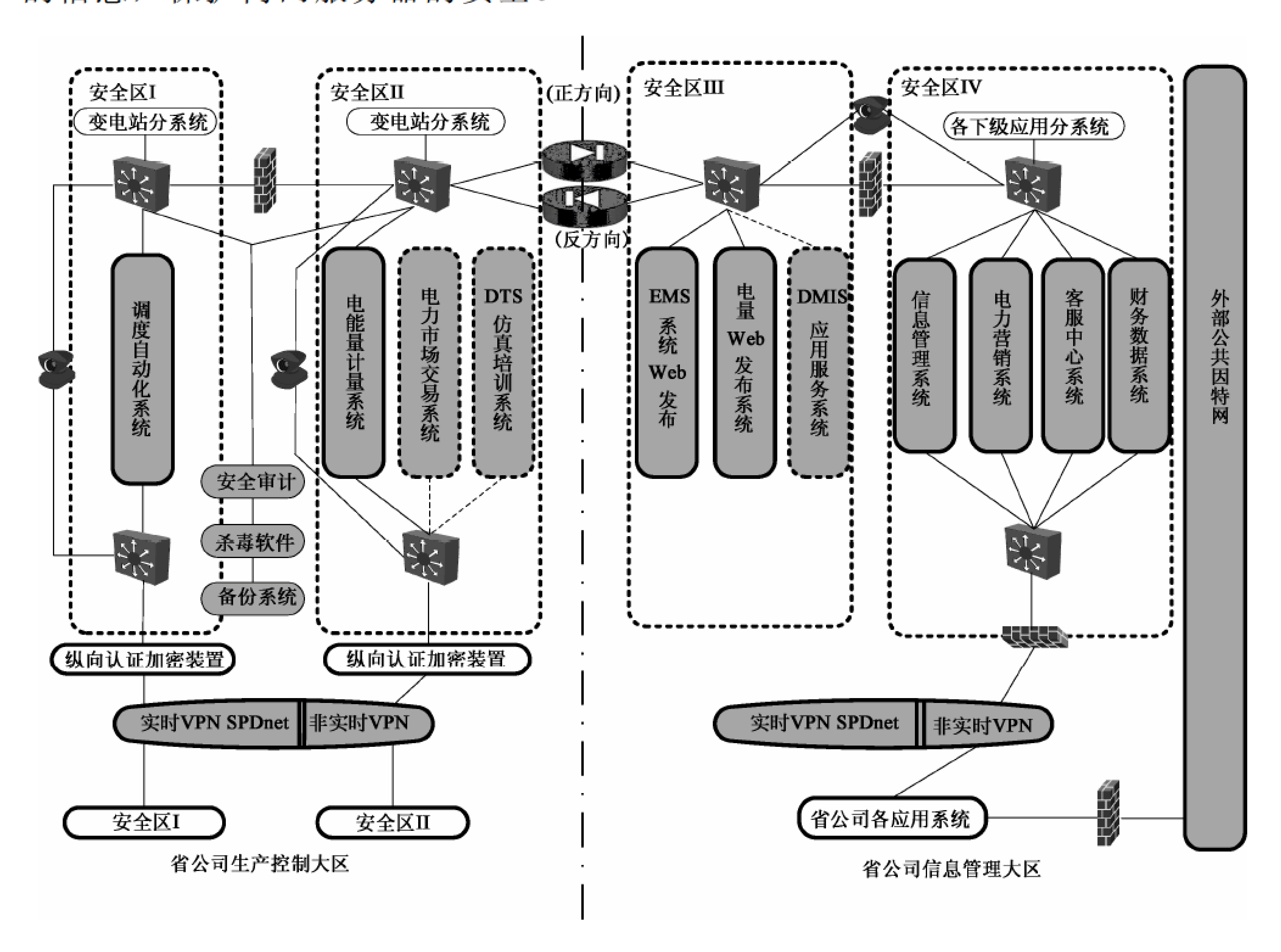


图 11-13 改造后的二次系统结构图

（2）针对红色代码、SQL 蠕虫、冲击波病毒、震荡波病毒等，提供了相应的升级包，可以在防火墙上阻断蠕虫对内部网络的攻击。

（3）实时监控功能可以随时帮助管理员查看各地市调与省调业务系统的连接状态、数据流量，以及监控网络流量的异常。

（4）支持 H.323 协议，满足视频会议、VOIP 等应用的要求。

（5）针对 III/IV 区远程办公的应用需求，防火墙可以通过添加 VPN 模块支持远程拨号接入，支持 NAT 穿越，并具有国家密码管理委员会办公室颁发的《商用密码产品技术鉴定证书》。对客户端身份的认证可以使用 USB KEY 认证方式，实现了双因子认证；支持 RADIUS 协议，可以与第三方认证服务器协同工作。

2）防病毒系统

病毒防护是调度系统与网络必须的安全措施。建议病毒的防护应该覆盖所有安全区（I、II、III、IV 区）的主机与工作站。对安全区 I 和 II 病毒特征码必须以离线的方式及时更新。技术要求如下：

（1）防病毒软件不仅要能保护文件，同时也要对各种服务器、PC、网关等所有计算机设备进行保护，而且能从邮件、FTP 文件、网页、软盘、光盘等所有可能带来病毒的信息源进行监控和病毒拦截。

（2）快速、有效地处理未知病毒，一旦防病毒软件发现一个文件可能携带

病毒，它应该有能力提供一种解决方法对该文件进行处理，以免系统或者文件受到未知病毒的破坏。

（3）提供强大的病毒实时监测能力，并尽可能少地占用系统资源。

（4）集中和方便地进行病毒定义码和扫描引擎的更新，既提供通过 Internet 从厂商的升级中心下载，同时也能从上一级病毒控制中心下载升级。

（5）应能智能安装、远程识别、管理方便、易于操作，统计和报表功能强大。

（6）客户端防病毒策略的强制定义和执行。

（7）提供多种报警手段，能通过电子邮件、打印机、寻呼机、手机或网络消息，传送各种病毒告警给携带病毒用户和系统管理员，并能提供标准输出，供其他系统对其告警信息二次开发。

3）入侵检测系统

为了实现 I/II 区、III/IV 区横向与纵向网络访问的监控与审计，计划在 I/II 区、III/IV 区分别部署网络入侵检测产品。网络入侵检测产品采用启明星辰的天阗入侵检测系统。该入侵检测产品拥有的技术特点如下：

（1）完善的管理控制体系，具体包括：

① 多层分级管理。天阗可灵活设置成与行政业务管理流程紧密结合的集中监控、多层管理的分级体系。通过策略下发机制，使上级部门能够统一全网的安全防护策略；通过信息上传机制，使上级部门能够及时了解和监控全网的安全状态。

② 灵活的更新和版本升级。天阗支持手动和自动的特征更新和软件版本升级，也可以在分级管理体系下由主控统一来完成。天阗的探测引擎同时支持通过 USB 口进行升级。

③ 全局预警。在天阗的多层分级管理体系下，可以实现把单点发生的重要事件自动预警到其他管理区域，使得各级管理员对于可能发生的重要安全事件具有提前的预警提示。利用全局预警通道，各级管理员也可以发送交互信息，交流对安全事件的处理经验。

④ 严格的权限管理。天阗可以设定多种分类权限供不同的人员使用，支持更为严格的多鉴别身份认证方式。同时在产品部署上支持事件监测、事件分析以及管理配置分布部署，从物理角度保证管理安全。

⑤ 时钟同步机制。天阗支持 NTP 服务进行时间同步，保证跨时区的部署条件下也能保持管理时间的一致性。

⑥ 支持多报警显示台。天阗提供了良好的多点监测机制，允许挂接多个报警显示中心，方便多个管理人员进行有效的报警观测。

⑦ 数据库维护管理。天阗支持多种数据库，如 MSSQL、Oracle 等，提供强大的数据库维护管理功能，支持快速入库，可以对历史数据进行自动、手动的备份、删除操作，还可以导入历史的备份数据。

⑧ 可扩展到入侵管理。天阗可以实现多种安全产品（如网络入侵检测、流量监测、漏洞扫描、主机入侵检测）的统一管理和协同关联。

（2）全面的入侵检测能力，具体包括：

① 多种技术结合防止漏报。天阗采用引擎高速捕包技术保证满负荷的报文捕获；天阗采用的高速树形匹配技术实现了一次匹配多个规则的模式，检测效率得以成倍的提高；天阗采用了 IP 碎片重组、TCP 流重组以及特殊应用编码解析等多种方式，应对躲避 IDS 检测的手法，如 WHISKER、FRAGROUTE 等攻击方式；天阗拥有了业界最为全面和更新速度最快的特征库，能够对通用的攻击方法和最新的流行攻击手段进行报警；采用预制漏洞机理分析方法定义特征，对未知攻击方式和变种攻击也能及时报警；采用行为关联分析技术，可以发现基于组合行为的复杂攻击。

② 多种措施降低误报。基于状态的协议分析和协议规则树，保证特征匹配的准确性；基于攻击过程的分析方法定义特征，可以识别攻击的状态，提供不同级别的事件报警信息；通过采集和关联攻击发送方和被攻击目标的信息，可以给出成功或失败的攻击事件明确标识；通过支持入侵管理，可以结合漏洞扫描结果来评估威胁的风险级别。

③ 多种机制限制滥报。天阗内置了状态检测机制，可以识别和处理类似“STICK”等的反 IDS 攻击，有效地避免了事件风暴的产生；天阗提供了多种可选的统计合并技术，可以对同一事件合并上报，减少报警量。

④ 自定义入侵检测规则。天阗提供了规范化的 VT++语言和向导定义模式，帮助用户自定义检测模式，扩充检测范围。

⑤ 全面兼容 CVE 和 CNCVE 标准。天阗通过了 CVE 严格的兼容性标准评审，并获得了最高级别的 CVE 兼容性认证（CVE Compatible），在入侵检测系统知识库上得到了国际权威组织的认可；同时，天阗也具有标准的 CNCVE 的对照。

（3）自适应检测策略管理，具体包括：

① 天阗提供多种不同分类方式的系统策略集，可以针对不同环境、不同应用以及关注目标选取最合适的检测策略。

② 天阗提供向导方式、已有策略集之间逻辑操作和在系统策略集上衍生等多种方式，方便用户自定义最佳使用的检测策略集，并支持策略集的导入和导出。

③ 天阗提供了灵活的策略编辑方式，确保用户在最短的时间内调整自己所需要的策略。

④ 天阗提供了动态策略调整模式，可以根据预设的事件发生频率来动态调整策略中应用的响应方式、合并条件以及过滤条件，从而减少报警日志量或者自动对高级事件调高相应级别。

⑤ 天阗支持虚拟引擎的划分，可以为不同网络对象制定适应性的检测策略，实现有效的入侵检测。

（4）可扩展的响应和联动。天阗具有丰富的可扩展事件响应方式，具体包括。

① 屏幕显示。

② 日志记录。

③ TCP KILLER 阻断。

④ 支持邮件方式远程报警、声音以及自定义程序报警。

⑤ 支持向网管发送 SNMP TRAP 信息。

⑥ 天阗通过自有 VIP 协议簇,可以充分实现和第三方安全产品以及网络设备的策略响应联动。

⑦ 防火墙联动。通过对天阗的联动通信标准的支持，防火墙业界主流的20 家以上的产品可以实现和天阗的联动，对外部发起的攻击行为进行阻断。

⑧ 交换机联动。天阗可以和港湾公司的智能安全系列交换机联动，根据策略指定动态关闭相应的交换机端口，可以防止蠕虫类事件的攻击扩散，进行内网安全防护。

（5）多样化日志分析报告，具体包括：

① 天阗分别为管理人员和入侵检测分析员提供了不同类型的日志分析手段和报告输出。

② 天阗为管理人员提供了常用的周期性统计模板，提供多类型 TOP10 的排名，管理人员可以直接利用，得出管理性的安全结论。

③ 天阗为入侵检测分析员提供了多种默认分析模板,根据这些模板可以获得多种分类的事件日志信息和交叉统计排名，既可以对事件详细追踪处理，也可以发现主要安全事件的焦点所在。

④ 天阗提供了多样化的日志过滤查询条件,用户可以进行自主定义习惯的查询模式，进行有效的日志分析查询，报表的题头、内容、字段可供用户自主调整。通过对于默认模板的选择和自定义过滤查询条件，用户可以进行自主制定多样化的分析报告模板并进行保存使用。天阗的报表可以手动、自动导出为多种常用格式（如 Word\Excel），并设置邮件定时发送报告功能。

（6）高度的自主安全保障，具体包括：

① 堡垒最容易从内部攻破，因此安全产品要保证自身的安全性尤其重要。天阗采取了多种先进措施保障自己的安全，并通过了国家 EAL3 级安全评测。

② 控制中心与所探测网段可以实现隔离部署，保证控制中心的自身安全管理。

③ 控制中心与探测引擎通信加密,探测器和控制中心互相认证,防止欺骗,防止日志、策略在传输过程中被篡改。

④ 探测引擎检测网口无 IP 地址，入侵者无法对消失在网络中的目标进行扫描和攻击，这样在网络中实现自身隐藏及带外管理；管理网口不开放额外连接端口，提高自身的隐藏性。

⑤ 探测引擎操作系统内核重新编译，并经过了特别的优化，不采用通用的TCP/IP 堆栈，避免通用 TCP/IP 堆栈的缺陷导致的安全漏洞。

⑥ 探测引擎具有 Watchdog 功能，确保系统的长期稳定运行。

（7）人性化界面功能操作。天阗在界面设计和功能上充分考虑了整体布局

美观性和用户操作习惯方便性，主要表现在以下几方面：

① 采用图形化拓扑结构显示产品组件之间的管理控制关系；

② 采用可定制的分窗口和事件树分类显示报警信息；

③ 提供向导操作模式，供用户按照规范的步骤进行准确操作；

④ 提供可定位的联机手册和具有详细的攻击、漏洞解释的安全信息手册，帮助用户参阅功能使用和事件查询。

（8）线速级的高性能处理。攻击特征流采用统一的 100 种标准的不同攻击样本，目标机器配置多种网络服务。网络背景流量采用专用发包设备来制造，以 0 背景流量为基准，测试入侵检测系统在不同的流量环境（包长）和不同连接背景下的检测能力。

4）漏洞扫描系统

网络安全评估与漏洞扫描可发现网络和主机系统的安全漏洞，并提供安全解决建议，且对全网进行安全配置检查。漏洞扫描产品采用启明星辰的天镜网络漏洞扫描与评估系统。该产品拥有的技术特点如下：

天镜网络漏洞扫描与评估系统是一套基于 Windows 平台的漏洞扫描软件，它包括了网络模拟攻击、漏洞检测、报告服务进程、提取对象信息、风险评估和安全建议等功能，帮助用户控制可能发生的安全事件，最大可能地消除安全隐患。该系统具有强大的漏洞检测能力和检测效率、贴切用户需求的功能定义、灵活多样的检测方式、详尽的漏洞修补方案和友好的报表系统，并支持在线升级。

天镜网络漏洞扫描与评估系统是一套工具软件，既可安装于台式计算机机置于网络中作为定期安全检查和风险报告的评估设备，也可安装于笔记本式计算机作为移动方式检查的便携工具。

5）隔离装置

为实现Ⅱ/Ⅲ区之间的正反向隔离需求，采用南瑞信息技术研究所研制的 SysKeeper-2000 网络安全隔离产品。

（1）正向型系统特点如下：

① 由两个高性能嵌入式微机及辅助装置形成安全隔离系统，嵌入式微处理器采用 RISC 体系结构，减少受攻击的概率；实现两个安全区之间的非网络方式的数据交换，并且采用安全算法保证安全隔离装置内外两个处理系统不同时连通。

② 安全隔离产品硬件供电采用的是国外进口开关电源，符合 EN 55022 class B，IEC 801-2、3、4、5、EN 60555-2、3EMC 标准，平均无故障时间达 64 223h。在 PCB 的设计中，加有线性稳压及滤波装置，并严格按照 EDA 对高频电路设计的要求，设计了单独的电源层与地层，进一步保证了整个电路板上电源的稳定性。

③ 支持双机热备：一台工作在主机位置，一台工作于备用位置，两台机器时刻进行通信并进行信息备份，一旦一台隔离设备出现故障时，或者处于

Watchdog 复位阶段，备机可以承担起主机的工作，以避免重要数据的丢失。

④ 严格的生产流程控制：南瑞网络安全隔离系列产品严格遵循 ISO 9000 2000 版质量认证体系，对每一台隔离产品的关键芯片和元器件进行产品老化试验，所有的隔离产品在出厂前必须经过 240h 以上的连续通电测试，确保每一台网络安全隔离产品运行的稳定性和硬件的高可靠性。

⑤ 支持双电源：在安全隔离设备中，设计有双电源。在工作的时候，一个电源作为主电源供电，一个做为辅电源备份，实现了主备电源的在线无缝切换，有效地提高整个电源工作的可靠性及延长整个系统的平均无故障工作时间。

⑥ 嵌入式 Linux 内核安全裁剪，内核中只包括用户管理、进程管理和 Socket 编程接口，裁剪掉 TCP/IP 协议栈和其他不需要的系统功能，进一步提高了系统安全性和抗攻击能力。

⑦ 支持系统告警：南瑞网络安全隔离装置支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可通过隔离装置专用的告警串口输出报警信息。

⑧ 物理上控制反向 FIFO 芯片的深度为 4B，保证从低安全区到高安全区的 TCP 应答禁止携带应用数据，大大增强了高安全区业务系统的安全性。在物理上实现了数据流的纯单向传输，数据只能从内网流向外网。

⑨ 安全隔离装置采用截断 TCP 连接的方法，剥离数据包中的 TCP/IP 头，将内网的纯数据通过单向数据通道 FIFO 发送到外网，同时只允许应用层不带任何数据的 TCP 包的控制信息传输到内网。

⑩ 采用综合过滤技术，在链路层截获数据包，然后根据用户的安全策略决定如何处理该数据包；实现了 MAC 与 IP 地址绑定，防止 IP 地址欺骗；支持静态地址映射（NAT）以及虚拟 IP 技术；具有可定制的应用层解析功能，支持应用层特殊标记识别，为用户提供一个全透明、安全、高效的隔离装置。

⑪ SysKeeper-2000 网络安全隔离产品采用独特的自适应技术，隔离设备没有 IP 地址，隐藏 MAC 地址，非法用户无法对隔离设备进行网络攻击，有效地提高了系统的安全性能。

⑫ 隔离设备采用 Motorola 高性能 RISC 体系结构 CPU，内核使用高效的过滤算法，充分发挥良好的硬件性能，采用两片 32 bit 高速传输芯片实现数据的高速安全传输，百兆状态下的有效网络吞吐率最高可达 70Mbit/s，不会造成网络通信的瓶颈。

⑬ 针对 I/II 区到 III 区通信内容规定，SysKeeper-2000 网络安全隔离设备提供了丰富的通信工具软件和 API 函数接口，方便用户进行二次系统隔离改造。

⑭ 隔离设备提供了友好的图形化用户界面，可以进行全新的可视化管理与配置。整个界面使用全中文化的设计，通过友好的图形化界面，网络管理员可以很容易地定制安全策略和对系统进行维护管理。

（2）反向型系统特点如下：

① 由两个高性能嵌入式微机及辅助装置形成安全隔离系统，嵌入式微处理

器采用 RISC 体系结构，减少受攻击的概率；实现两个安全区之间的非网络方式的数据交换，并且采用安全算法保证安全隔离装置内外两个处理系统不同时连通。

② 安全隔离装置硬件供电采用的是国外进口开关电源，符合 EN 55022 class B，IEC 801-2、3、4、5，EN 60555-2、3EMC 标准，平均无故障时间达 64 223h。在 PCB 的设计中，加有线性稳压及滤波装置，并严格按照 EDA 对高频电路设计的要求，设计了单独的电源层与地层，进一步保证了整个电路板上电源的稳定性。

③ 支持双机热备：一台工作在主机位置，一台工作于备用位置，两台机器时刻进行通信并进行信息备份，一旦一台隔离设备出现故障时，或者处于 Watchdog 复位阶段，备机可以承担起主机的工作，以避免重要数据的丢失。

④ 严格的生产流程控制：南瑞网络安全隔离系列产品严格遵循 ISO 9000 2000 版质量认证体系，对每一台隔离产品的关键芯片和元器件进行产品老化试验，所有的隔离产品在出厂前必须经过 240h 以上的连续通电测试，确保每一台网络安全隔离产品运行的稳定性和硬件的高可靠性。

⑤ 支持双电源：在安全隔离产品中，设计有双电源。在工作的时候，一个电源作为主电源供电，一个作为辅电源备份，实现了主备电源的在线无缝切换，有效地提高整个电源工作的可靠性及延长整个系统的平均无故障工作时间。

⑥ 嵌入式 Linux 内核安全裁剪，内核中只包括用户管理、进程管理和 Socket 编程接口，裁剪掉 TCP/IP 协议栈和其他不需要的系统功能，进一步提高了系统安全性和抗攻击能力。

⑦ 采用基于数字证书的数字签名技术，在数据的发送端对需要发送的数据进行签名，然后发给专用反向隔离装置；隔离装置收到数据后进行签名验证，并根据用户对数据的定义检查数据文件的格式和内容，支持通用的数据类型和记录分隔符；反向隔离装置将处理过的数据发送给内网的数据接收程序。

⑧ 编码转换技术：SysKeeper-2000 网络安全隔离装置（反向型）提供的专用发送软件在发送文本文件数据时，自动将半角字符转换为全角字符，反向隔离装置都会按照编码范围正确的识别，保证进入内网的数据为纯文本数据。

⑨ 完善的密钥管理机制：网络安全隔离装置（反向型）提供基于 RSA 公私密钥对的数字签名和采用电力专用加密算法进行数字加密的功能。进行 RSA 运算时，为了保证密钥的安全性，提供已知密钥的 ID 号使用密钥的功能，密钥仅存在于网络安全隔离装置（反向型）的安全存储区中，与应用系统隔离，不能通过任何非法手段进行访问，极大地提高了数据交换的安全性。

⑩ 支持系统告警：南瑞网络安全隔离装置（反向型）支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可通过隔离装置专用的告警串口输出报警信息。

⑪ 采用综合过滤技术，在链路层截获数据包，然后根据用户的安全策略决定如何处理该数据包；实现了 MAC 与 IP 地址绑定，防止 IP 地址欺骗；支持

静态地址映射（NAT）以及虚拟 IP 技术；割断穿透性的 TCP 连接；具有可定制的应用层解析功能，支持应用层特殊标记识别，为用户提供一个全透明、安全、高效的隔离装置。

⑫ 网络安全隔离装置(反向型)采用 Motorola 高性能 RISC 体系结构 CPU，采用电力对称加密算法及 RSA 公私密钥算法实现数据加解密、数字签名、身份认证等功能，保证数据的安全传输。在 1024 bit 模长下，RSA 数字签名速度为 150 次/s，密文数据包吞吐率为 20Mbit/s（50 条安全策略，1024B 报文长度）。

⑬ 为了使隔离设备达到预期的安全效果，经过网络安全隔离装置(反向型)进行数据传输的软件必须按照《全国电力二次系统安全防护总体方案》的规定进行开发。针对 III 区到 I/II 区通信内容规定，南瑞 SysKeeper-2000 网络安全隔离装置（反向型）提供专用文件传输软件（实现数字签名、编码转换、内容有效性检查和数字签名功能），方便用户进行二次系统安全隔离改造。

⑭ 南瑞 SysKeeper-2000 网络安全隔离装置（反向型）提供了基于数字证书的图形化用户界面，通过反向隔离装置的专用智能 IC 卡读写器进行身份认证，保证配置管理的安全性。整个界面使用全中文化的设计，通过友好的图形化界面，网络管理员可以很容易地定制安全策略和对系统进行维护管理，用户只需进行简单的培训就可以完成对隔离设备的管理与配置。

4. 安全管理体系

1）安全管理组织结构

本着“谁主管，谁负责”的原则，电业局调度中心负责本地电力监控系统及地区电力调度数据网络的安全管理。

为落实电力二次系统安全防护的安全责任，电业局已成立二次系统安全防护小组，由电业局分管领导负责，包括调度中心领导、生技部领导、自动化科专责、网络专责、安全专责、各业务部门计算机专责，统筹安排所辖范围内的安全防护工作部署。

2）安全管理制度建设

健全的安全管理制度是日常管理的规范和基准，应根据二次系统的实际情况，建立以下日常管理制度：

（1）机房及重要场所门禁制度。

（2）各应用系统维护管理制度，包括电能量管理系统、电力模拟市场技术支持系统、负荷控制系统、通信监控系统、能量计费系统、集控中心 SCADA 系统、DMIS 系统等的维护管理制度。

（3）各安全防范系统维护管理制度，包括数据网络平台、各种安全隔离装置（防火墙、安全隔离装置等）、入侵检测系统、防病毒系统等的维护管理制度。

（4）调度中心计算机病毒防范制度。

（5）安全防护岗位职责制度。

（6）各专业系统备份与恢复管理制度。

（7）安全评估安全审计管理制度。

（8）职工定期安全培训制度。

（9）数字证书/口令管理制度。

3）工程实施的安全管理

（1）新建的电力二次系统工程的设计必须符合国家、行业的有关安全防护的标准、法规、法令、规定、导则等。

（2）对新建的电力二次系统必须在建设过程中进行安全评估，并根据评估结果制定安全策略。

（3）新接入地区电力调度数据网络的结点、设备和应用系统，须经负责地区调度中心核准，并送上一级电力调度机构备案。

（4）电力二次系统的安全防护方案必须经过上级主管单位的审查、批准，完工后必须经过上级有关部门验收。

（5）电力二次系统安全防护方案的实施必须严格遵守电监会 5 号令以及本公司的有关规定，保证部署的安全装置的可用性指标达到 99.99%。

4）设备、应用及服务的接入管理

（1）在已经配置安全体系的电力二次系统中接入任何新的设备和应用及服务，均必须立案申请，经过本单位的安全专责以及本单位的主管领导审查批准后，方可在安全专责的监管下实施接入。

（2）电力二次系统的安全区 I 及安全区 II 中的工作站、服务器原则上不得开通拨号功能。若确需开通拨号服务，必须配置强认证机制，否则该应用必须与安全区 I 及安全区 II 彻底隔离。

（3）在所有电力二次系统的安全区 I 及安全区 II 中的任何工作站、服务器均严格禁止以各种方式开通与互联网、其他安全区及任何外部网络的连接。

（4）电力二次系统的安全区 I 及安全区 II 中的 PC 及其他微机原则上应该将软盘驱动、光盘驱动、USB 接口拆除，以防止病毒的传播。若个别 PC 确有必要插接 USB-key，应该严格管理。

（5）接入电力二次系统的安全区 I 及安全区 II 中的通用安全产品必须使用经过国家有关安全部门认证的国产产品；接入电力二次系统的专用安全产品必须使用国产产品并经过有关电力主管部门的认证，并应该优先选用经过有关电力主管部门推荐的优秀安全产品。

5）日常运行管理

（1）日常运行管理的具体内容如下：

① 所有操作人员必须经过严格的审查，并且具有相应的技术能力才可以上岗。

② 操作人员必须采取分级管理制度，针对不同的电力二次系统，对不同的用户实体、不同的使用人员赋予相应的访问权限和操作权限。

③ 所有授权操作人员的操作必须严格遵守操作规范。

④ 授权操作人员违反操作规范，应立即从计算机系统中删除其操作权限，

并追究其责任。

⑤ 授权操作人员辞职或岗位调动，应从计算机系统中删除其操作权限。

⑥ 所有操作人员申请资料以及操作人员撤销过程进行日志存档。

（2）日常维护工作管理的具体内容如下：

① 系统权限管理：针对不同的应用系统、用户实体、操作人员设置数据库信息的访问权限，应用系统功能的选择权限。系统提供对各种应用、各类用户实体、不同担任者的集中式的权限管理。

② 系统信息备份：提供保障信息存储安全的规范，备份的信息要和系统分开存放，必要时要做硬拷贝。

③ 系统服务维护：提供对各种业务流程的处理和管理方法的维护手段。维护的内容包括服务规则、服务参数设置和服务处理模式。服务维护应提供专门的界面，避免直接通过源程序或数据库进行操作。

④ 系统数据库维护：通过数据库系统提供的维护工具进行。操作人员要观察数据库系统运行的状况，及时对用户实体、数据库、数据空间进行调整。系统应能够在发生故障时恢复。

⑤ 系统服务器维护：通过服务器硬件厂商提供的维护工具进行，包括对服务器系统内部硬件资源的状态检测、对外部设备的检测、硬件障碍的恢复等。

⑥ 操作系统管理：通过操作系统厂商提供的维护工具进行，包括对系统运行的状态进行检测、对内部和外部设备的运行状态进行监视、对资源配置进行调整。

⑦ 系统网络管理：通过网管工作站的网管软件进行。运用设置在工作站上的软件可以对系统上的智能设备如工作站、主机、网络设备进行集中检测、维护和控制。

⑧ 应用软件维护：应用软件开发完成应当按照国家软件工程相关技术标准提交文档资料。对应用软件因功能要求变化或软件出错的维护应当制定详细的可溯性文档，如问题分析、处理方法、处理结果等。

⑨ 系统日志维护：所有操作人员的操作和系统的变化必须记录到日志中，并且该日志只能由具有许可授权的管理人员才可以管理。

⑩ 对已投运且已建立安全体系的系统定期进行漏洞扫描，以便及时发现系统的安全漏洞。

⑪ 对安全体系的各种日志（如入侵检测日志等）审计结果进行认真地研究以发现系统的安全漏洞。

⑫ 定期分析各系统的安全风险及漏洞、分析当前黑客非法入侵的特点，根据分析及时调整安全策略。

⑬ 病毒防护：在 MIS 系统 Web 服务器上设立专门的页面发布病毒及黑客攻击的敌情报告以及最新的病毒库和相应的升级的防病毒软件。

⑭ 及时了解相关系统软件（操作系统、数据库系统、各种工具软件）漏洞发布信息，及时获得补救措施或软件补丁对软件进行加固。

（3）应急处理工作：应急处理工作处理一些突发性事件，维护工作必须制定相应的应急处理策略，包括紧急事件的报告程序、紧急事件的处理过程和方法等。应急处理工作包括以下内容：

① 系统软件安全漏洞的维护：一方面针对系统软件中出现的安全漏洞，及时同软件供应商联系；另一方面跟踪软件供应商的安全漏洞发布信息，了解相关软件漏洞发布信息，及时获得对系统安全漏洞的补救措施或软件补丁。

② 发现系统正被黑客攻击的维护：要求每一个业务系统都制定相关问题处理措施的应急方案，按照既定方案实施系统维护，如可以根据不同情况分别采用加强保护、中断对方连接、反跟踪及其他处理措施。

③ 灾难恢复维护：系统运行可能会因为自然或人为的原因遭到破坏，应当制定相应问题处理的应急方案，按照既定的方案实施系统恢复维护，如采用立即完全恢复、部分恢复、启用备份系统恢复（保护现场）等。

11.4.4 一网多业务终端虚拟化隔离案例

1. 项目建设背景与需求

银行业作为信息密集型企业，对于信息系统、网络平台和信息资源的依赖程度相当高，信息化平台已经成为银行的脊柱。作为处于市场的高增长期的行业，银行业的高速成长、产业格局的形成和商业模式的不断变化对信息化提出了很高的要求。

银行业正面临比以往更严峻的形势——信息网络空间的斗争日趋尖锐、境内外网络违法犯罪活动呈快速递增趋势、恶意代码和网络攻击呈多样化局面等。近年来，银行业界内发生了多起信息安全事件，美国花旗银行遭遇黑客攻击导致客户数据泄密、巴西中央银行网站被攻击瘫痪、银行员工兜售客户信息等，这些事件给业界敲响了警钟。

客户信息盗取产业链的不断壮大，如何保障数据的安全性，对银行业而言显得越来越重要。银行涉密数据已不再仅仅是银行自身的问题，甚至有可能成为一个社会问题，有着极大的不良影响，其主要风险体现如下：

（1）在银行内部，曾出现员工倒卖客户信息以获取高额利润，或利用手里调用资金权限进行网络赌博等非法活动，给银行造成了巨额损失。

（2）在银行外部，一种叫做“病毒集团”的机构，以病毒方式侵入银行内部 PC，悄无声息的扫描 PC 和内网服务器上敏感数据，从而导致数据被动泄密，盗取客户信息以谋取经济利益已经形成一条产业链。

（3）大多数银行生产网和互联网做了严格的物理隔离，但是在办公网和互联网之间，由于高昂的建设成本（从网络、服务器、终端 PC 完全复制一套），却鲜有物理隔离。因此，互联网病毒很容易通过终端以各种方式侵入到办公网，获取数据。

（4）尽管各行在互联网出口部署防火墙、IPS、IDS、网关杀毒等安全防御设备，加强安全防御，然而这些传统的终端安全防护技术，均是被动处理网络威胁，“封、堵、拦”的手段已经无法应对技术性和隐蔽性强的木马病毒，无法从根本上彻底解决终端数据安全问题，导致行内安全风险依然居高不下。

结合银行业目前实际情况，PC 终端承载了内部数据交换和外部数据沟通的重要任务，终端和系统相连，是整个银行网络中的支撑点，如同人体的神经末梢，一旦终端的安全防护被突破，则给连接 PC 的系统、网络造成无法预料的威胁。

因此，如何能够通过一台办公网的 PC 终端使用户高效地实现多种业务的操作（互联网、内网 OA 等应用、内网敏感数据的访问），同时提供有效的安全隔离控制手段，避免不同业务之间的病毒感染、木马入侵、数据泄密等风险成为了 XX 银行本次项目建设的关键。

概括成一句话就是：在实现终端多业务数据安全的同时，兼顾用户使用体验和效率，以及方案成本。

2．项目建设方案介绍

XX 银行在测试了包括桌面/应用虚拟化技术、安全沙盒隔离技术、DPL 技术等大量技术手段之后，最终选择了安全沙盒作为项目建设的核心技术，提供从服务器—PC 终端端到端的安全域划分。

在一台终端上通过多沙盒的虚拟安全桌面划分不同的业务安全域：默认桌面访问内部普通业务系统，上网安全桌面访问互联网业务，防泄密安全桌面访问内部敏感数据业务系统。三个桌面之间实现有效的数据隔离、网络隔离、病毒隔离，防止互联网风险进入内网，防止内部敏感数据泄露到互联网。

数据泄露前，用户在不同的安全域里访问相关的数据，若用户在安全桌面内引入了互联网安全风险，如下载了病毒或木马程序，随着安全桌面系统的注销，安全桌面内部的访问痕迹都会随之清除，并不会影响计算机系统本身，更不会扩散到内网。同时，安全桌面系统隔离计算机本身的文件系统，用户在使用安全桌面访问互联网时，敏感数据梧不会过互联网泄露出去。

在事中，多沙盒系统的安全桌面结合 AC 上网行为管理网关和 VSP 加密隔离网关，以规范用户的身份和网络使用行为，确保安全制度的落地和执行。在事后，多沙盒系统提供了完整的追溯审计功能，在快速定位泄密事件当事人的同时，协助管理人员发现安全制度的执行漏洞，以实现安全技术与管理制度的协调和统一。

此外，再与原有的数据内容保护技术相结合，在数据生命周期过程中，数据安全主要通过事前的数据加密、访问身份控制，事中的传输链路加密、权限审批、安全告警，以及事后审计、水印溯源等方式来实现，提供了一个全方位的数据保护。

最终，XX 银行一网多业务终端虚拟化隔离方案，在数据安全性和用户易

用性之间、虚拟化先进性与投资回报比之间找到了最合理的平衡点，让数据安全与现有的 IT 投资得到了最佳的融合过渡。

3．项目实施部署效果

XX 银行一网多业务终端虚拟化隔离方案部署以来，在安全性、用户易用性、运维简便性、TCO 投入产出比等方面取得了很好的效果。

1）虚拟化隔离安全性高，避免了更新滞后性

与传统的防病毒软件基于病毒特征库识别的实时查杀和磁盘扫描技术不一样，沙盒虚拟化隔离技术并不对病毒木马本身进行查杀，而是将注册表、文件系统、系统服务进程、网络、外设硬件等的关键组件和涉密数据通过虚拟化隔离保护起来，不再需要实时更新病毒特征库，既减少了终端计算机的日常维护，又从另一个角度补充了防病毒软件的滞后性不足。

同时，沙盒安全桌面可以与上网行为管理网关配合，能够对用户访问的互联网站点、上传的文件内容、通过即时通信软件传递的信息和文件、邮件的附件等进行透明的监管和审计，能够从技术上确保安全部门的上网行为管理制度的落地执行，避免终端用户受到钓鱼邮件或恶意广告的影响而无意间引入了病毒风险，同时也可以结合实时告警制度，当用户尝试将机密文件外传时，系统给出告警提示，对有意访问非法站点的终端用户形成一种无形的震慑力，提高了终端用户对上网安全管理制度的执行力。

2）对用户的使用习惯影响小，易用性高

与多计算机物理隔离、双硬盘物理隔离卡等传统方案不一样，对应着不同安全域的安全桌面方案可以随时进行切换，无须 1s 就能够切换到另一个安全域的虚拟桌面，无须重新启动操作系统，也无须维护多个客户端计算机，方便快捷，简单易用。

应用程序在沙盒安全桌面内运行时，可以直接使用客户计算机的硬件资源，运行速度与直接在真实计算机桌面中运行完全一样，即使是在安全桌面内运行如 3D 图像设计等对显卡性能要求很高的工作站程序，对用户的终端易用性体验也毫无影响。

3）轻量级的虚拟化隔离方案，易部署推广

与基于硬件虚拟化的虚拟机方案，或基于计算集中化的桌面虚拟化方案对客户端计算机或终端服务器的高性能要求不同，多沙盒虚拟化隔离方案是基于应用层实现的轻量级虚拟化方案，既不需要依赖高性能的终端服务器部署，也不需要高性能的客户端计算机，一台配备 512MB 内存和单核 CPU 的普通 PC 就能够流畅地运行沙盒安全桌面，能够将目前业界内绝大部分现有计算机复用起来，无须对现有用户计算机或服务器进行大面积的更新换代，也无须对 IT 部门的维护管理工作产生额外的压力或挑战。

在网络部署方面，多沙盒虚拟化安全方案无须改动现有的网络部署方案，所需设备都支持旁挂、网关方式部署，只需要部署在安全域网络的边界处即可，

对现有网络部署没有影响，易于快速实现上线部署。

4）投资产出比高，极大地节省了 TCO

多沙盒虚拟化安全方案无论是在前期的设备投资方面，还是后续的部署实施成本以及运维成本上，与其他方案相比都取得了最好的投入产出比。

首先，在设备投资方面，与物理隔离方案、应用虚拟化等方案项目相比，多沙盒方案的投资成本节约了 80%以上，如图 11-14 所示。

其次，在实施部署过程中，多沙盒方案无需改变行内原有的网络，实施周期短，在最小程度下改变员工的使用习惯，并在一周内让员工接受了此改变，因此从方案推广和实施上凸显了极大的优势，至少节省了 40%的成本。

最后，在运维过程中，多沙盒系统与现有的用户身份认证系统无缝对接，具有自动告警、实时监控等功能，极大地减轻了安全策略的部署、维护工作量。此外，系统部署后，病毒事件数量减少了 90%以上，极大地减轻了基层 IT 人员的 PC 运维工作量，如图 11-15 所示。

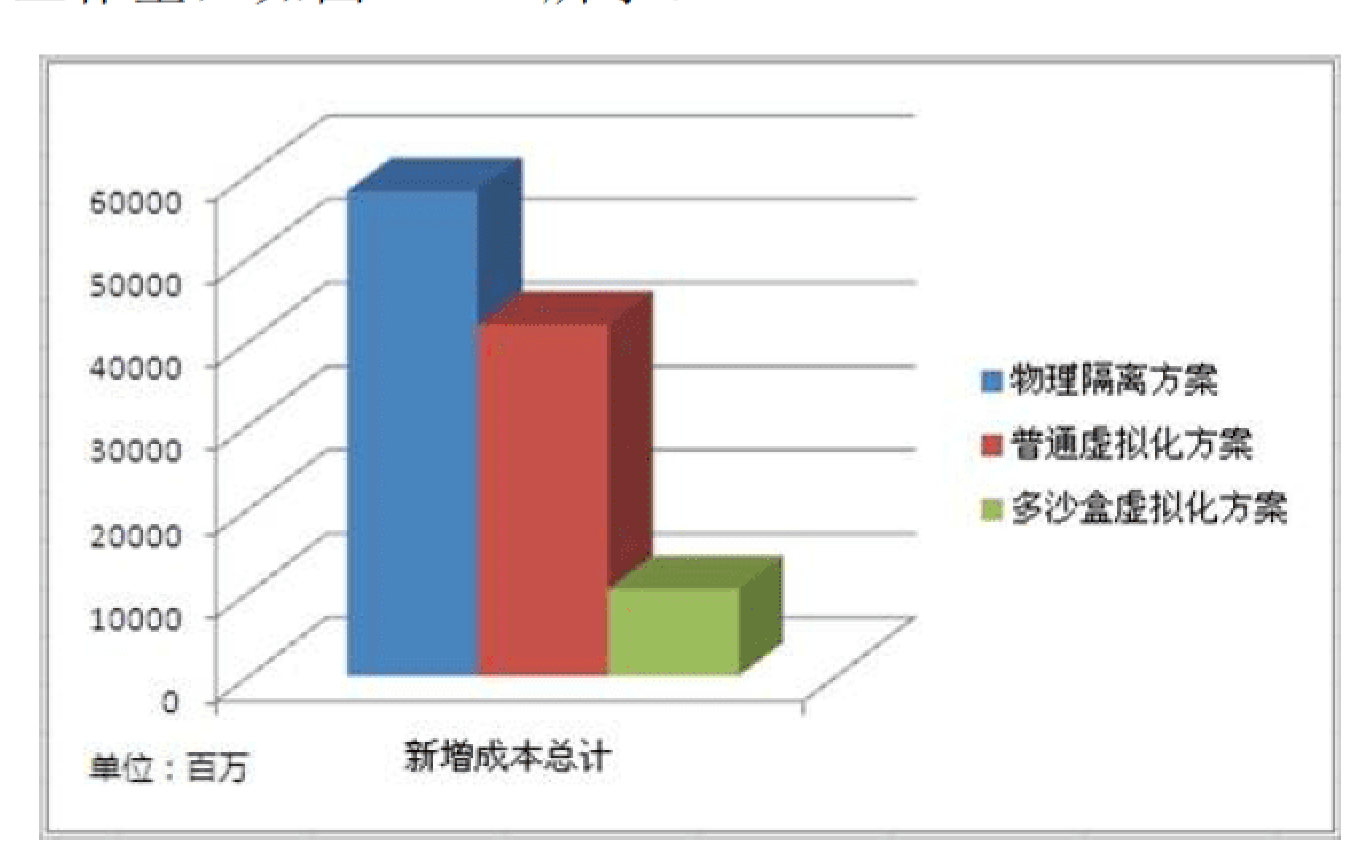


图 11-14　多沙盒方案的投资分析

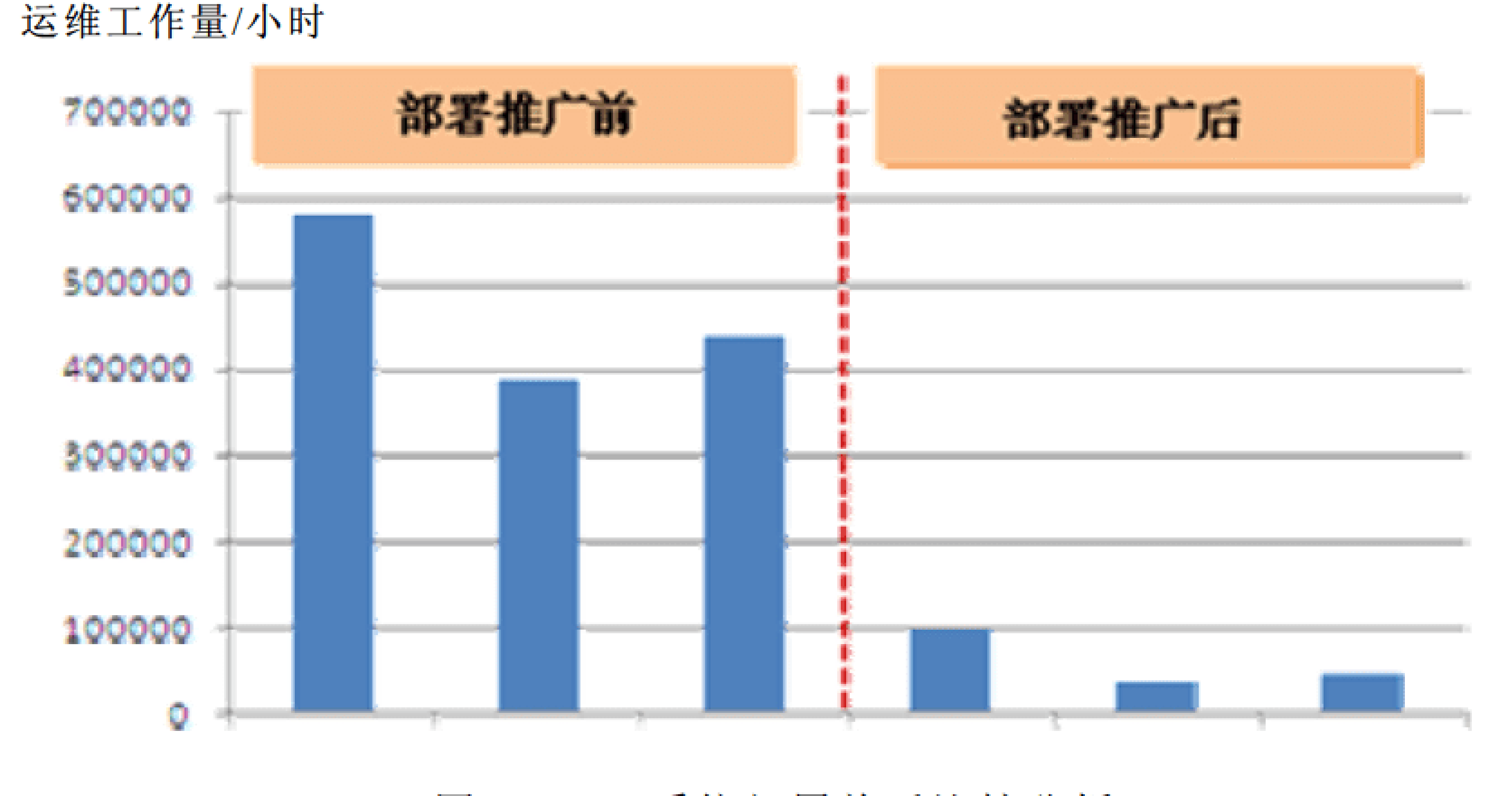


图 11-15　系统部署前后比较分析

参 考 文 献

[1] P. Mell, T Grance. “The NIST Definition of Cloud Computing”, http://csrc.nist.gov/groups/SNS/cloud-computing/ .

[2] IDC Enterprise Panel, “Cloud Computing Survey”, Aug. 2008, http://blogs.idc.com/ie/?p=210 .

[3] Jon Brodkin, “Gartner: Seven Cloud Computing Security Risks”, July 2008, http://www.infoworld.com/d/ security-central/gartner-seven-cloud-computing-security-risks-853.

[4] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing v2.1,” Dec. 2009, http://www.cloudsecurityalliance.org/.

[5] Information Systems Audit and Control Association, “Cloud Computing: Business Benefits With security, Governance and Assurance Perspectives” Mar. 2009, http://www.isaca.org/Template.cfm?Section=Research2&CONTENTID=53050&TEMPLATE=/ContentManagement/ContentDisplay.cfm.

[6] European Network and Information Security Agency, “Cloud Computing Information Assurance Framework”, Mar. 2010, http://www.enisa.europa.eu/act/rm/files/deliverables/ cloud-computing- information-assuranceframe work/?searchterm=cloud.

[7] S. Curry, J. Darbyshire, D. W. Fisher, et al, “RSA Security Breif: Infrastructure Security”, http://www.rsa.com/innovation/docs/CCOM_BRF_0310.pdf.

[8] http://blog.sina.com.cn/alexalei.

[9] 《云计算安全架构》，中国通信标准化协会《通信技术与标准》，2010，9.

[10] 王惠莅，杨晨，杨建军. 云计算安全和标准研究[J]. 信息技术与标准化，2012（05）.

[11] IBM 信息安全白皮书.

[12] 公安部，信息安全等级保护培训教材，2007.8.

[13] 曾庆凯，许峰，张有东. 信息安全体系结构[M]. 北京：电子工业出版社，2010，8.

[14] 工业和信息化部电子科学技术情报研究所，2010 世界网络与信息安全发展年度报告.

[15] 雷万云. 云计算——企业信息化建设策略与实践[M]，北京：清华大学出版社，2010.

[16] 雷万云. 云计算——技术、平台与应用案例[M]. 北京：清华出版社，2011.

[17] 雷万云. 信息化与信息管理实践之道[M]. 北京：清华大学出版社，2012.

[18] 雷万云. 中国企业必须考虑云计算[J]. 管理学家杂志，2012，9.

[19] 雷万云. 云计算产业为何遭遇 CIO 冷遇？[J]. 中国经济和信息化杂志，2012，14.